Preface

Audience

This guide is for the networking professional managing the Cisco Metro Ethernet (ME) 3800X and 3600X switch, hereafter referred to as the switch. We assume that you are familiar with the concepts and terminology of Ethernet and local area networking. If you are interested in more training and education in these areas, learning opportunities including training courses, self-study options, seminars, and career certifications programs are available on the Cisco Training & Events web page:


Purpose

This guide provides procedures for using the commands that have been created or changed for use with the Cisco ME 3800X and ME 3600X switch. It does not provide detailed information about these commands. For detailed information about these commands, see the Cisco ME 3800X and ME 3600X Switch Command Reference for this release. For information about the standard Cisco IOS commands, see the Cisco IOS documentation available from this URL:


This guide does not describe system messages you might encounter or how to install your switch. For more information, see the Cisco ME 3800X and ME 3600X Switch System Message Guide for this release and the Cisco ME 3800X and ME 3600X Switch Hardware Installation Guide.

For the latest 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 and cautions use these conventions and symbols:

<table>
<thead>
<tr>
<th>Note</th>
<th>Means reader take note. Notes contain helpful suggestions or references to materials not contained in this manual.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caution</td>
<td>Means reader be careful. 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 these Cisco.com sites:

- ME 3800X switch:
- ME 3600X switch:

**Note**

Before installing, configuring, or upgrading the switch, see these documents:

- For initial configuration information, see the “Configuring the Switch with the CLI-Based Setup Program” appendix in the hardware installation guide.
- For upgrading information, see the “Downloading Software” section in the release notes.

- Release Notes for the Cisco ME 3800X and ME 3600X Switch

**Note**

See the release notes on Cisco.com for the latest information.

- Cisco ME 3800X and ME 3600X Switch Software Configuration Guide
- Cisco ME 3800X and ME 3600X Switch Command Reference
- Cisco ME 3800X and ME 3600X System Message Guide
- Cisco ME 3800X and ME 3600X Switch Hardware Installation Guide
- Cisco ME 3800X and ME 3600X Switch Getting Started Guide
- Installation Note for the Cisco ME 3800X and ME 3600X Switch Power Supply and Fan Modules
- Regulatory Compliance and Safety Information for the Cisco ME 3800X and ME 3600X Switches
Cisco Confidential - Release 15.1(2)EY - EFT DRAFT

- Cisco Small Form-Factor Pluggable Modules Installation Notes
- Cisco CWDM GBIC and CWDM SFP 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 CWDM SFP Transceiver 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 these topics about the Cisco Metro Ethernet (ME) 3800X and 3600X switch software:

- **Software Licenses and Features**, page 1-1
- **Features**, page 1-2
- **Limitation**, page 1-11
- **Where to Go Next**, page 1-11

In this document, IP refers to IP Version 4 (IPv4).

Software Licenses and Features

If you have a service support contract and order a software license or if you order a switch, you receive the universal software image, available in crypto and noncrypto versions. If you do not have a service support contract, such as a SMARTnet contract, download the image from Cisco.com.

The ME 3600X supports these licenses:

- Metro IP access is the universal image.
- Advanced Metro IP access license.
- 10 Gigabit Ethernet upgrade license—enables 10 Gigabit Ethernet on the SFP+ uplink ports.

For differences in feature support for each license, see Table 1-1 and Table 1-2 on page 1-10.

The ME 3800X supports these licenses plus a scaled license that can be installed with any of these licenses to increase the supported values for that license, for example, more MAC addresses, VLANs, IPv4 routes, and so on.

- Metro Ethernet services is the universal image.
- Metro IP service license.
- Metro Aggregation services license.

For differences in feature support for each license, see Table 1-2 and Table 1-4 on page 1-10.

To install a software image, see the switch release notes and the “Working with the Cisco IOS File System, Configuration Files, and Software Images” chapter in the software configuration guide.

To install a software license, see the “Cisco IOS Software Activation Tasks and Commands” chapter in the Cisco IOS Software Activation Configuration Guide:

Features

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. Other features require a specific license. For more information, see the release notes for this release.

- Performance Features, page 1-2
- Management Options, page 1-3
- Manageability Features, page 1-3
- Availability Features, page 1-5
- VLAN Features, page 1-5
- Security Features, page 1-6
- Quality of Service and Class of Service Features, page 1-7
- Layer 2 Virtual Private Network Services, page 1-7
- Layer 3 Features, page 1-8
- Layer 3 VPN Services, page 1-8
- Monitoring Features, page 1-9

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 interfaces that enables the interface to automatically detect the required cable connection type (straight-through or crossover) and to configure the connection appropriately
- Support for 9800 byte frames on routed ports and switch ports at all speeds: 10/100/1000/10000 Mb/s.
- IEEE 802.3x flow control on all ports (the switch does not send pause frames)
- EtherChannel for enhanced fault tolerance
- Port Aggregation Protocol (PAgP) and Link Aggregation Control Protocol (LACP) for automatic creation of EtherChannel links
- Forwarding of Layer 2 and Layer 3 packets at Gigabit and 10 Gigabit line rates
- 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
- Internet Group Management Protocol (IGMP) snooping for IGMP versions 1, 2, and 3 on switchports for efficiently forwarding multimedia and multicast traffic
- IGMP report suppression for sending only one IGMP report per multicast router query to the multicast devices (supported only for IGMPv1 or IGMPv2 queries)
- IGMP snooping querier support to configure switch to generate periodic IGMP General Query messages
• IGMP throttling for configuring the action when the maximum number of entries is in the IGMP forwarding table
• IGMP configurable leave timer to configure the leave latency for the network.
• RADIUS server load balancing to allow access and authentication requests to be distributed evenly across a server group.

Management Options

• CLI—The Cisco IOS software supports desktop- and multilayer-switching 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.”
• Cisco Configuration Engine—The Cisco Configuration Engine is a network management device that works with embedded Cisco IOS CNS Agents in the switch software. 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 using Cisco IOS agents, see Chapter 4, “Configuring Cisco IOS Configuration Engine.”
• SNMP—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. For more information about using SNMP, see Chapter 25, “Configuring SNMP.”

Manageability Features

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

• Support for synchronous Ethernet (SyncE) to synchronize and send clock information to remote sites on the network for the same clock accuracy, stability, and traceability in the network.
• Support for Ethernet Virtual Connections (EVCs), conceptual service pipes for point-to-point or multipoint-to-multipoint paths within the service provider network, for bridge domains, and for Ethernet Flow Points (EFPs) logical interfaces that connect bridge domains to a physical ports in a switch. Some software features are supported on ports only or on EFPs only.
• Support for DHCP for configuration of switch information (such as IP address, default gateway, hostname, and Domain Name System [DNS] and TFTP server names)
• DHCP relay for forwarding User Datagram Protocol (UDP) broadcasts, including IP address requests, from DHCP clients
• DHCP server for automatic assignment of IP addresses and other DHCP options to IP hosts
• DHCP-based autoconfiguration and image update to download a specified configuration a new image to a large number of switches
• DHCP server port-based address allocation for the preassignment of an IP address to a switch port
Features

• 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
• 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 (supported on NNIs by default, can be enabled on ENIs, not supported on UNIs)
• Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED) for interoperability with third-party IP phones
• Support for the LLDP-MED location TLV that provides location information from the switch to the endpoint device
• Network Time Protocol (NTP) for providing a consistent time stamp 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 Secure Shell (SSH) connections for multiple CLI-based sessions over the network (requires the cryptographic versions of the switch software).
• In-band management access through SNMP Versions 1, 2c, 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
• Out-of-band management access through the Ethernet management port to a PC
• User-defined command macros for creating custom switch configurations for simplified deployment across multiple switches
• 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 switches, and IEEE 802.3ah Ethernet OAM discovery, link monitoring, remote fault detection, and remote loopback, and IEEE 802.3ah Ethernet OAM discovery, link monitoring, remote fault detection, and remote loopback
• Configuration replacement and rollback to replace the running configuration on a switch with any saved Cisco IOS configuration file
• 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.
Availability 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 1000 supported spanning-tree instances
  - 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
- 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 modes:
  - Port Fast for eliminating the forwarding delay by enabling a spanning-tree port to immediately transition from the blocking state to the forwarding state
  - Bridge protocol data unit (BPDU) guard for shutting down Port Fast-enabled ports that receive BPDUs
  - BPDU filtering for preventing a Port Fast-enabled ports 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
- Flex Link Layer 2 interfaces to back up one another as an alternative to STP for basic link redundancy in a nonloop network with preemptive switchover and bidirectional fast convergence, also referred to as the MAC address-table move update feature
- Flex Link Multicast Fast Convergence to reduce the multicast traffic convergence time after a Flex Link failure
- Support for Resilient Ethernet Protocol (REP) for improved convergence times and network loop prevention without the use of spanning tree
- Support for REP edge ports with the no-neighbor option when the neighbor port is not REP-capable
- HSRP for Layer 3 router redundancy
- Equal-cost routing for link-level and switch-level redundancy (requires metro IP access image)

VLAN Features

- Support for up to 4094 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 allowed by the IEEE 802.1Q standard
• 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

• 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. The switch CPU continues to send and receive control protocol frames.

• VLAN Flex Link Load Balancing on physical interfaces 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.

Security Features

Switch Security

Note

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

• Password-protected access (read-only and read-write access) to management interfaces for protection against unauthorized configuration changes

• Configuration file security so that only authenticated and authorized users have access to the configuration file, preventing users from accessing the configuration file by using the password recovery process

• Multilevel security for a choice of security level, notification, and resulting actions

• MAC security option for limiting and identifying MAC addresses of the stations allowed to access Ethernet Flow Points (EFPs)

• MAC security aging to set the aging time for secure addresses on a service instance

• LLDP (Link Layer Discovery Protocol) and LLDPP-MED (Media Extensions)—Adds support for IEEE 802.1AB link layer discovery protocol for interoperability in multi-vendor networks. Switches exchange speed, duplex, and power settings with end devices such as IP Phones.

• 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 versions of the switch software)

Network Security

• 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/UDP headers
• Source and destination MAC-based ACLs for filtering non-IP traffic
• 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.

Quality of Service and Class of Service Features

• Cisco modular quality of service (QoS) command-line (MQC) implementation
• Three levels of hierarchical output queueing
• Classification based on IP precedence, Differentiated Services Code Point (DSCP), and IEEE 802.1p class of service (CoS) packet fields, ACL lookup, and multiprotocol label switching (MPLS) Experimental bits, or assigning a discard class or QoS label for output classification
• Policing
  – One-rate policing based on average rate and burst rate for a policer
  – Two-color policing that allows different actions for packets that conform to or exceed the rate
  – Ingress two-rate, three-color policing for individual or aggregate policers
• Weighted tail drop (WTD) as the congestion-avoidance mechanism for managing the queue lengths and providing drop precedences for different traffic classifications
• Queuing and Scheduling
  – Deficit round robin traffic shaping to mix packets from all queues to minimize traffic burst
  – Class-based traffic shaping to specify a maximum permitted average rate for a traffic class
  – Port shaping to specify the maximum permitted average rate for a port
  – Class-based weighted queuing (CBWFQ) to control bandwidth to a traffic class
  – WTD to adjust queue size for a specified traffic class
  – Low-latency priority queuing to allow preferential treatment to certain traffic
• Per-port, per-VLAN QoS to control traffic carried on a user-specified VLAN for a given interface. You can use hierarchical policy maps for per-VLAN classification and apply the per-port, per-VLAN hierarchical policy maps to trunk ports.

Layer 2 Virtual Private Network Services

• IEEE 802.1Q tunneling on EFPs to enable service providers to offer multiple point Layer 2 VPN services to customers
• Layer 2 protocol tunneling on EFPs to enable customers to control protocols, such as BPDU, CDP, VTP, LLDP, MSTP, PAgP, LACP, and UDLD protocols, to be tunneled across service-provider networks.
• 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.
• 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.
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
  - EIGRP
  - BGP Version 4
  - IS-IS dynamic routing
  - BFD protocol Bidirectional Forwarding Detection (BFD) Protocol to detect forwarding-path failures for OSPF, IS-IS, BGP, EIGRP, or HSRP routing protocols
- 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
- 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
- Support for the SSM PIM protocol to optimize multicast applications, such as video
- DHCP relay for forwarding UDP broadcasts, including IP address requests, from DHCP clients

Layer 3 VPN Services

- Multiple VPN routing/forwarding (multi-VRF) instances in customer edge devices (multi-VRF CE) to allow service providers to support multiple virtual private networks (VPNs) and overlap IP addresses between VPNs
- VRF and EIGRP compatibility
- VRF-aware 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.
- 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 devices to allow service providers to support multiple VPNs and to overlap IP addresses between VPNs.
- Support for MPLS traffic engineering and fast reroute link protection for rerouting LSP traffic around a failed link
Monitoring Features

- Switch LEDs that provide port- and switch-level status
- Configurable external alarm inputs
- 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
- 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
- Time Domain Reflector (TDR) to diagnose and resolve cabling problems on copper Ethernet 10/100 ports
- SFP module diagnostic management interface to monitor physical or operational status of an SFP module
- Online diagnostics to test the hardware functionality switch while the switch is connected to a live network
- On-board failure logging (OBFL) to collect information about the switch and the power supplies connected to it
- IP Service Level Agreements (IP SLAs) support to measure network performance by using active traffic monitoring
- IP SLAs for Metro Ethernet using IEEE 802.1ag Ethernet Operation, Administration, and Maintenance (OAM) capability to validate connectivity, jitter, and latency in a metro Ethernet network

Feature Support per License

Table 1-1 ME 3600X Supported Features per License

<table>
<thead>
<tr>
<th>Metro IP Access (Universal Image)</th>
<th>Advanced Metro IP Access license</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Basic Layer 2 features (including 802.1Q)</td>
<td>• All features in the Metro IP Access image</td>
</tr>
<tr>
<td>• EVCs</td>
<td>• MPLS</td>
</tr>
<tr>
<td>• IPv4 routing (RIP, OSFP, EIGRP, IS-IS, and BGP) and BFD</td>
<td>• MPLS traffic engineering and Fast Reroute</td>
</tr>
<tr>
<td>• Multicast routing (PIM, DM, SSM and SSM mapping)</td>
<td>• MPLS OAM</td>
</tr>
<tr>
<td>• Ethernet OAM (802.1ag, 802.3ah, and E-LMI),</td>
<td>• MPLS VPN</td>
</tr>
<tr>
<td>• MST, REP, Flex Links</td>
<td>• Ethernet over MPLS (EoMPLS)</td>
</tr>
<tr>
<td>• Synchronous Ethernet with Ethernet Synchronization Messaging Channel (ESMC)</td>
<td>• Pseudowire redundancy</td>
</tr>
<tr>
<td>• Multi VRF-CE (VRF-Lite) with service awareness (ARP, ping, SNMP, syslog, traceroute, FTP and TFTP)</td>
<td>• Virtual Private LAN Services (VPLS)</td>
</tr>
</tbody>
</table>
### Table 1-2 ME 3600X License Scaling

<table>
<thead>
<tr>
<th>Supported feature</th>
<th>Metro IP Access</th>
<th>Advanced Metro IP Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC addresses</td>
<td>8 K</td>
<td>16 K</td>
</tr>
<tr>
<td>IPv4 routes</td>
<td>20 K</td>
<td>20 K</td>
</tr>
<tr>
<td>IPv4 multicast groups and routes</td>
<td>1 K</td>
<td>1 K</td>
</tr>
<tr>
<td>Layer 2 multicast entries</td>
<td>1 K</td>
<td>1 K</td>
</tr>
<tr>
<td>Bridge domains</td>
<td>4 K</td>
<td>4 K</td>
</tr>
<tr>
<td>ACL entries</td>
<td>2 K</td>
<td>2 K</td>
</tr>
</tbody>
</table>

### Table 1-3 ME 3800X Supported Features per License

<table>
<thead>
<tr>
<th>Metro Ethernet Services (Universal Image)</th>
<th>Metro IP Services license</th>
<th>Metro Aggregation Services license</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Basic Layer 2 features (including 802.1d and 802.1Q)</td>
<td>• All features in the Metro Ethernet Services image</td>
<td>• All features in the Metro IP Services license</td>
</tr>
<tr>
<td>• EVCs</td>
<td>• IPv4 routing (RIP, OSPF, EIGRP, IS-IS, and BGP)</td>
<td>• MPLS</td>
</tr>
<tr>
<td>• Ethernet OAM (802.1ag, 802.3ah, and E-LMI)</td>
<td>• BFD</td>
<td>• MPLS traffic engineering and Fast Reroute</td>
</tr>
<tr>
<td>• MST, REP, Flex Links</td>
<td>• Multicast routing (PIM, DM, SSM and SSM mapping)</td>
<td>• MPLS OAM</td>
</tr>
<tr>
<td>• Synchronous Ethernet with Ethernet Synchronization Messaging Channel (ESMC)</td>
<td>• Multi VRF-CE (VRF-Lite) with service awareness (ARP, ping, SNMP, syslog, traceroute, FTP and TFTP)</td>
<td>• MPLS VPN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ethernet over MPLS (EoMPLS)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Pseudowire redundancy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Virtual Private LAN Services (VPLS)</td>
</tr>
</tbody>
</table>

### Table 1-4 ME 3800X License Scaling

<table>
<thead>
<tr>
<th>Supported feature</th>
<th>Metro Services</th>
<th>Scaled Metro Services</th>
<th>Metro IP Services</th>
<th>Scaled Metro IP Services</th>
<th>Metro Aggregation Services</th>
<th>Scaled Metro Aggregation Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC table addresses</td>
<td>64 K</td>
<td>128 K</td>
<td>32 K</td>
<td>64 K</td>
<td>128 K</td>
<td>256 K</td>
</tr>
<tr>
<td>IPv4 routes</td>
<td>1 K</td>
<td>1 K</td>
<td>42 K</td>
<td>80 K</td>
<td>24 K</td>
<td>32 K</td>
</tr>
<tr>
<td>IPv4 multicast groups and routes</td>
<td>0</td>
<td>0</td>
<td>2 K</td>
<td>4 K</td>
<td>2 K</td>
<td>4 K</td>
</tr>
<tr>
<td>Layer 2 multicast entries</td>
<td>2 K</td>
<td>4 K</td>
<td>2 K</td>
<td>2 K</td>
<td>2 K</td>
<td>4 K</td>
</tr>
<tr>
<td>Bridge domains</td>
<td>4 K</td>
<td>4 K</td>
<td>2 K</td>
<td>4 K</td>
<td>4 K</td>
<td>8 K</td>
</tr>
<tr>
<td>ACL entries</td>
<td>4 K</td>
<td>8 K</td>
<td>4 K</td>
<td>8 K</td>
<td>4 K</td>
<td>16 K</td>
</tr>
</tbody>
</table>
Limitation

The IPv6 Provider Edge (6PE) and IPv6 VPN Provider Edge (6VPE) commands are not supported in this release.

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”
CHAPTER 2

Using the Command-Line Interface

This chapter describes the Cisco IOS command-line interface (CLI) and how to use it to configure your Cisco ME 3800X and 3600X 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 hostname `Switch`. 
Understanding Command Modes

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>Switch&gt;</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>Switch#</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>Switch(config)#</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>Switch(config-vlan)#</td>
<td>To exit to global configuration mode, enter the <code>exit</code> command.</td>
<td>Use this mode to configure VLAN parameters.</td>
</tr>
<tr>
<td>Interface</td>
<td>While in global configuration mode, enter the <code>interface</code> command (with a specific interface).</td>
<td>Switch(config-if)#</td>
<td>To exit to global configuration mode, enter <code>exit</code>.</td>
<td>Use this mode to configure parameters for the Ethernet ports.</td>
</tr>
<tr>
<td>configuration</td>
<td></td>
<td></td>
<td></td>
<td>For information about defining interfaces, see the “Using Interface Configuration Mode” section on page 10-6.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To configure multiple interfaces with the same parameters, see the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>“Configuring a Range of Interfaces” section on page 10-7.</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>Switch(config-line)#</td>
<td>To exit to global configuration mode, enter <code>exit</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 guide 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.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>Switch# dir?</td>
</tr>
<tr>
<td></td>
<td>dir disable disconnect</td>
</tr>
<tr>
<td>abbreviated-command-entry&lt;tab&gt;</td>
<td>Complete a partial command name.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>Switch# sh conf&lt;tab&gt;</td>
</tr>
<tr>
<td></td>
<td>Switch# show configuration</td>
</tr>
<tr>
<td>?</td>
<td>List all commands available for a particular command mode.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>Switch&gt; ?</td>
</tr>
<tr>
<td>command ?</td>
<td>List the associated keywords for a command.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# cdp holdtime ?</td>
</tr>
<tr>
<td></td>
<td>&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: 'show con'</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 appear.</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 appear.</td>
</tr>
<tr>
<td>% Invalid input detected at '^' 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 appear.</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><code>show history</code></td>
<td>While in privileged EXEC mode, list the last several commands that you just entered. The number of commands that appear is controlled by the setting of the <code>terminal history</code> global configuration command and the <code>history</code> 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.

- 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 the Delete or Backspace key.**
- Delete the character at the cursor.

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

- **Press Ctrl-K.**
- Delete all characters from the cursor to the beginning 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.

#### Note
- The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including `show` command output. You can use the Return and Space bar keystrokes whenever you see the More prompt.

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

<table>
<thead>
<tr>
<th>Capability</th>
<th>Keystroke(^1)</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete entries if you make a mistake or change your mind.</td>
<td>Press the Delete or Backspace key.</td>
<td>Erase the character to the left of the cursor.</td>
</tr>
<tr>
<td></td>
<td>Press the Delete or Backspace key.</td>
<td>Erase the character to the left of the cursor.</td>
</tr>
<tr>
<td></td>
<td>Press Ctrl-D.</td>
<td>Delete the character at the cursor.</td>
</tr>
<tr>
<td></td>
<td>Press Ctrl-K.</td>
<td>Delete all characters from the cursor to the end of the command line.</td>
</tr>
<tr>
<td></td>
<td>Press Ctrl-U or Ctrl-X.</td>
<td>Delete all characters from the cursor to the beginning of the command line.</td>
</tr>
<tr>
<td></td>
<td>Press Ctrl-W.</td>
<td>Delete the word to the left of the cursor.</td>
</tr>
<tr>
<td></td>
<td>Press Esc D.</td>
<td>Delete from the cursor to the end of the word.</td>
</tr>
<tr>
<td>Capitalize or lowercase words or capitalize a set of letters.</td>
<td>Press Esc C.</td>
<td>Capitalize at the cursor.</td>
</tr>
<tr>
<td></td>
<td>Press Esc L.</td>
<td>Change the word at the cursor to lowercase.</td>
</tr>
<tr>
<td></td>
<td>Press Esc U.</td>
<td>Capitalize letters from the cursor to the end of the word.</td>
</tr>
<tr>
<td>Designate a particular keystroke as an executable command, perhaps as a shortcut.</td>
<td>Press Ctrl-V or Esc Q.</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 Return key.</td>
<td>Scroll down one line.</td>
</tr>
<tr>
<td></td>
<td>Press the Space bar.</td>
<td>Scroll down one screen.</td>
</tr>
<tr>
<td>Redisplay the current command line if the switch suddenly sends a message to your screen.</td>
<td>Press Ctrl-L or Ctrl-R.</td>
<td>Redisplay the current command line.</td>
</tr>
</tbody>
</table>

\(^1\) The arrow keys function only on ANSI-compatible terminals such as VT100s.
## 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` appear.

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
GigabitEthernet0/1 is up, line protocol is down
GigabitEthernet0/2 is up, line protocol is up
```
Accessing the CLI

You can access the CLI through a console connection, through Telnet, or by using the browser.

Accessing 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 9-6.

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 9-6. 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 9-36. 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 Cisco Metro Ethernet (ME) 3800X and 3600X 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 Software Documentation, 12.2 Mainline Release, Command References, Volume 1 of 3: Addressing and Services.

This chapter consists of these sections:

- Understanding the Boot Process, page 3-1
- Assigning Switch Information, page 3-3
- Checking and Saving the Running Configuration, page 3-16
- Modifying the Startup Configuration, page 3-17
- Scheduling a Reload of the Software Image, page 3-21

Information in this chapter about configuring IP addresses and DHCP is specific to IP Version 4 (IPv4).

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 functions:

- 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 a Lost or Forgotten Password” section on page 37-2.

**Note**
You can disable password recovery. For more information, see the “Disabling Password Recovery” section on page 9-5.

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.

**Note**
If the data bits option is set to 8, set the parity option to none.
• Stop bits default is 1.
• Parity settings default is none.

**Initial Configuration**

The switch is set to automatically boot to the bootloader. When the bootloader is fully operational, the prompt appears:

```
switch:
```

See the “Boot Loader Commands” appendix in the command reference for this release for descriptions of the available commands. To manually boot an image from flash memory, enter:

```
switch: boot flash: image name
```

If you do not know the image name on the flash memory, you can retrieve the name with this command:

```
switch: dir flash:
Directory of flash:/
2  -rwx  2072      <date>               multiple-fs
3  -rwx  5         <date>               private-config.text
4  -rwx  3045      <date>               config.text
5  drwx  512       <date>               me380x-universal-mz.122-52.1.127.EY
16920593 bytes available (41011183 bytes used)
```
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). For more information about the setup program, see the “Configuring the Switch with the CLI-Based Setup Program” appendix in 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.

These sections contain this configuration information:
- Default Switch Information, page 3-3
- Understanding DHCP-Based Autoconfiguration, page 3-4
- Manually Assigning IP Information, page 3-15

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>
</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**

```
Switch A
```

- DHCPDISCOVER (broadcast)
- DHCPOFFER (unicast)
- DHCPREQUEST (broadcast)
- DHCPACK (unicast)
- DHCPACK (unicast)

```
DHCP server
```

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

In a DHCPREQUEST broadcast message, the client returns a formal request for the offered configuration information to the DHCP server. The formal request is broadcast so that all other DHCP servers that received the DHCPDISCOVER broadcast message from the client can reclaim the IP addresses that they offered to the client.
The DHCP server confirms that the IP address has been allocated to the client by returning a DHCPACK unicast message to the client. With this message, the client and server are bound, and the client uses configuration information received from the server. The amount of information the switch receives depends on how you configure the DHCP server. For more information, see the “Configuring the TFTP Server” section on page 3-7.

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 unicsats, 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 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 over write 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 autoconfiguration 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).
Assigning Switch Information

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.)

**Note**
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.
- 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 contain this configuration information:

- DHCP Server Configuration Guidelines, page 3-7
- Configuring the TFTP Server, page 3-7
- Configuring the DNS, page 3-8
- Configuring the Relay Device, page 3-8
- Obtaining Configuration Files, page 3-9
- Example Configuration, page 3-10
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
Assigning Switch Information

Chapter 3  Assigning the Switch IP Address and Default Gateway

Assigning Switch Information

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:

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

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

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

On interface 20.0.0.1:

```
router(config-if)# ip helper-address 10.0.0.1
```
If the switch is acting as the relay device, configure the interface as a routed port. For more information, see the “Routed Ports” section on page 10-3 and the “Configuring Layer 3 Interfaces” section on page 10-19.

Figure 3-2  Relay Device Used in Autoconfiguration

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, it 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, it 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.
Assigning Switch Information

Chapter 3      Assigning the Switch IP Address and Default Gateway

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 ciscort.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.

![DHCP-Based Autoconfiguration Network Example](image)

Table 3-2 shows the configuration of the reserved leases on the DHCP server.

<table>
<thead>
<tr>
<th></th>
<th>Switch A</th>
<th>Switch B</th>
<th>Switch C</th>
<th>Switch D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Binding key (hardware address)</td>
<td>00e0.9f1e.2001</td>
<td>00e0.9f1e.2002</td>
<td>00e0.9f1e.2003</td>
<td>00e0.9f1e.2004</td>
</tr>
<tr>
<td>IP address</td>
<td>10.0.0.21</td>
<td>10.0.0.22</td>
<td>10.0.0.23</td>
<td>10.0.0.24</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Router address</td>
<td>10.0.0.10</td>
<td>10.0.0.10</td>
<td>10.0.0.10</td>
<td>10.0.0.10</td>
</tr>
<tr>
<td>DNS server address</td>
<td>10.0.0.2</td>
<td>10.0.0.2</td>
<td>10.0.0.2</td>
<td>10.0.0.2</td>
</tr>
<tr>
<td>TFTP server name</td>
<td>tftpserver or 10.0.0.3</td>
<td>tftpserver or 10.0.0.3</td>
<td>tftpserver or 10.0.0.3</td>
<td>tftpserver or 10.0.0.3</td>
</tr>
<tr>
<td>Boot filename (configuration file) (optional)</td>
<td>switcha-config</td>
<td>switchb-config</td>
<td>switchc-config</td>
<td>switchd-config</td>
</tr>
<tr>
<td>Hostname (optional)</td>
<td>switcha</td>
<td>switchb</td>
<td>switchc</td>
<td>switchd</td>
</tr>
</tbody>
</table>
DNS Server Configuration

The DNS server maps the TFTP server name `tftpserver` 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-config 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-config`, `switchb-config`, and so forth) as shown in this display:

```
prompt> cd /tftpserver/work/
prompt> ls
network-config
switcha-config
switchb-config
switchc-config
switchd-config
prompt> cat network-config
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-config file from the base directory of the TFTP server.
- It adds the contents of the network-config file to its host table.
- It reads its host table by indexing its IP address 10.0.0.21 to its hostname (switcha).
- It reads the configuration file that corresponds to its hostname; for example, it reads `switch1-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><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ip dhcp pool poolname</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>bootfile filename</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>network network-number mask \ prefix-length</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>default-router address</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>option 150 address</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>tftp-server flash:filename.text</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>no switchport</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>ip address address mask</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

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

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp)# network 10.10.10.0 255.255.255.0
Switch(config-dhcp)# bootfile config-boot.text
Switch(config-dhcp)# default-router 10.10.10.1
Switch(config-dhcp)# option 150 10.10.1.1
Switch(config-dhcp)# exit
Switch(config)# tftp-server flash:config-boot.text
Switch(config)# interface gigabitethernet0/4
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1 255.255.255.0
Switch(config-if)# end
```
Assigning Switch Information

Chapter 3      Assigning the Switch IP Address and Default Gateway

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.

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. 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>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip dhcp pool poolname</td>
<td>Create a name for the DHCP server address pool and enter DHCP pool configuration mode.</td>
</tr>
<tr>
<td>Step 3 bootfile filename</td>
<td>Specify the name of the file that is used as a boot image.</td>
</tr>
<tr>
<td>Step 4 network network-number mask prefix-length</td>
<td>Specify the subnet network number and mask of the DHCP address pool. Note The prefix length specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).</td>
</tr>
<tr>
<td>Step 5 default-router address</td>
<td>Specify the IP address of the default router for a DHCP client.</td>
</tr>
<tr>
<td>Step 6 option 150 address</td>
<td>Specify the IP address of the TFTP server.</td>
</tr>
<tr>
<td>Step 7 option 125 hex</td>
<td>Specify the path to the text file that describes the path to the image file.</td>
</tr>
<tr>
<td>Step 8 copy tftp flash filename.txt</td>
<td>Upload the text file to the switch.</td>
</tr>
<tr>
<td>Step 9 copy tftp flash imagename.tar</td>
<td>Upload the tarfile for the new image to the switch.</td>
</tr>
<tr>
<td>Step 10 exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 11 tftp-server flash:config.text</td>
<td>Specify the Cisco IOS configuration file on the TFTP server.</td>
</tr>
<tr>
<td>Step 12 tftp-server flash:imagename.tar</td>
<td>Specify the image name on the TFTP server.</td>
</tr>
<tr>
<td>Step 13 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>Step 14 interface interface-id</td>
<td>Specify the address of the client that will receive the configuration file.</td>
</tr>
<tr>
<td>Step 15 no switchport</td>
<td>Put the interface into Layer 3 mode.</td>
</tr>
<tr>
<td>Step 16 ip address address mask</td>
<td>Specify the IP address and mask for the interface.</td>
</tr>
<tr>
<td>Step 17 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 18 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 switch as a DHCP server so it downloads a configuration file:

```
Switch# config 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)# option 125 hex
0000.0009.0a05.0b66.7574.6f69.6e73.7461.6c6c.5e64.686370
```
Assigning Switch Information

Chapter 3      Assigning the Switch IP Address and Default Gateway

Assigning Switch Information

Switch(dhcp-config)# exit
Switch(config)# tftp-server flash:config-boot.text
Switch(config)# tftp-server flash:-image-name-mz.122-44.3.SE.tar
Switch(config)# tftp-server flash:boot-config.text
Switch(config)# tftp-server flash: autoinstall_dhcp
Switch(config)# interface gigabitEthernet0/4
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>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:

Switch# configure terminal
Switch(config)# boot host dhcp
Switch(config)# boot host retry timeout 300
Switch(config)# banner config-save ^C Caution - Saving Configuration File to NVRAM May Cause You to NoLonger Automatically Download Configuration Files at Reboot^C
Switch(config)# vlan 99
Switch(config-vlan)# interface vlan 99
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch# show boot
BOOT path-list:
  Config file:    flash:/config.text
  Private Config file: flash:/private-config.text
  Enable Break:   no
  Manual Boot:    no
  HELPER path-list:
  NVRAM/Config file buffer size: 32768
  Timeout for Config Download: 300 seconds
  Config Download via DHCP: enabled (next boot: enabled)
Manually Assigning IP Information

Beginning in privileged EXEC mode, follow these steps to manually assign IP information to a switch virtual interface (SVI). You can also manually assign IP information to a port if you first put the port into Layer 3 mode by using the `no switchport` command.

<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 vlan vlan-id</code></td>
<td>Enter interface configuration mode, and enter the VLAN to which the IP information is assigned. The range is 1 to 4094; do not enter leading zeros.</td>
</tr>
<tr>
<td>3</td>
<td><code>ip address ip-address subnet-mask</code></td>
<td>Enter the IP address and subnet mask.</td>
</tr>
<tr>
<td>4</td>
<td><code>exit</code></td>
<td>Return to global configuration mode.</td>
</tr>
</tbody>
</table>
| 5      | `ip default-gateway ip-address` | Enter the IP address of the next-hop router interface that is directly connected to the switch where a default gateway is being configured. The default gateway receives IP packets with unresolved destination IP addresses from the switch. Once the default gateway is configured, the switch has connectivity to the remote networks with which a host needs to communicate.  
Note When your switch is configured to route with IP, it does not need to have a default gateway set. |
| 6      | `end`                            | Return to privileged EXEC mode.                                          |
| 7      | `show interfaces vlan vlan-id`   | Verify the configured IP address.                                       |
| 8      | `show ip redirects`              | Verify the configured default gateway.                                  |
| 9      | `copy running-config startup-config` | (Optional) Save your entries in the configuration file.                  |

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.”
Checking and Saving the Running Configuration

You can check the configuration settings you entered or changes you made by entering this privileged EXEC command:

```
Switch# show running-config
Building configuration...

Current configuration : 1817 bytes
!
version 15.1
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Switch
!
!
no aaa new-model
authentication mac-move permit
ip subnet-zero
!
license boot level AdvancedMetroIPAccess
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 2,10
!
interface GigabitEthernet0
  no ip address
  shutdown
  negotiation auto
!
interface GigabitEthernet0/1
  port-type nni
!
interface GigabitEthernet0/2
  port-type nni
!
interface GigabitEthernet0/3
  port-type nni
!
interface TenGigabitEthernet0/1
  port-type nni
!
interface TenGigabitEthernet0/2
  port-type nni
!
interface Vlan1
  no ip address
  shutdown
!
```
ip classless
ip http server
!
!
line con 0
   speed 115200
line vty 5 15
!
End

To store the configuration or changes you have made to your startup configuration in flash memory, enter this privileged EXEC command:

Switch# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...

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 from which to copy the configuration file, see Appendix B, “Working with the Cisco IOS File System, Configuration Files, and Software Images.”

## Modifying the Startup Configuration

- Default Boot Configuration, page 3-18
- Automatically Downloading a Configuration File, page 3-18
- Booting Manually, page 3-19
- Booting a Specific Software Image, page 3-19
- Controlling Environment Variables, page 3-20

See also Appendix B, “Working with the Cisco IOS File System, Configuration Files, and Software Images,” for information about switch configuration files.
Chapter 3  Assigning the Switch IP Address and Default Gateway

Default Boot Configuration

Table 3-3  Default Boot Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system software image</td>
<td>The switch attempts to automatically boot the system using information in the BOOT environment variable. If the 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. The Cisco IOS image is stored in a directory that has the same name as the image file (excluding the .bin extension). In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory.</td>
</tr>
<tr>
<td>Configuration file</td>
<td>Configured switches use the config.text file stored on the system board in flash memory. A new switch has no configuration file.</td>
</tr>
</tbody>
</table>

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 3-4.

Specifying the Filename to Read and Write the System Configuration

By default, the Cisco 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 will be 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 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| Step 2 boot config-file flash:/file-url | Specify the configuration file to load during the next boot cycle.  
For file-url, specify the path (directory) and the configuration filename.  
Filenames and directory names are case sensitive. |
| Step 3 end                   | Return to privileged EXEC mode.                                                                   |
| Step 4 show boot             | Verify your entries.  
The boot config-file global configuration command changes the setting of the CONFIG_FILE environment variable. |
| Step 5 copy running-config startup-config | (Optional) Save your entries in the configuration file.  
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</td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td>Command</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>boot manual</strong></td>
</tr>
<tr>
<td>Command</td>
<td>Enable the switch to manually boot during the next boot cycle.</td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>end</strong></td>
</tr>
<tr>
<td>Command</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>show boot</strong></td>
</tr>
<tr>
<td>Command</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Command</td>
<td>The <strong>boot manual</strong> global command changes the setting of the</td>
</tr>
<tr>
<td>Command</td>
<td>MANUAL_BOOT environment variable.</td>
</tr>
<tr>
<td>Command</td>
<td>The next time you reboot the system, the switch is in boot loader</td>
</tr>
<tr>
<td>Command</td>
<td>mode, shown by the <strong>switch: prompt</strong>. To boot the system, use the</td>
</tr>
<tr>
<td>Command</td>
<td><strong>boot filesystem:file-url</strong> boot loader command.</td>
</tr>
<tr>
<td>Command</td>
<td>• For <strong>filesystem</strong>: use <strong>flash</strong>: for the system board flash device.</td>
</tr>
<tr>
<td>Command</td>
<td>• For <strong>file-url</strong>, specify the path (directory) and the name of the</td>
</tr>
<tr>
<td>Command</td>
<td>bootable image.</td>
</tr>
<tr>
<td>Command</td>
<td>Filenames and directory names are case sensitive.</td>
</tr>
<tr>
<td>Step 5</td>
<td><strong>copy running-config startup-config</strong></td>
</tr>
<tr>
<td>Command</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

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</td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td>Command</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>boot system filesystem:file-url</strong></td>
</tr>
<tr>
<td>Command</td>
<td>Configure the switch to boot a specific image in flash memory during</td>
</tr>
<tr>
<td>Command</td>
<td>the next boot cycle.</td>
</tr>
<tr>
<td>Command</td>
<td>• For <strong>filesystem</strong>: use <strong>flash</strong>: for the system board flash device.</td>
</tr>
<tr>
<td>Command</td>
<td>• For <strong>file-url</strong>, specify the path (directory) and the name of the</td>
</tr>
<tr>
<td>Command</td>
<td>bootable image.</td>
</tr>
<tr>
<td>Command</td>
<td>Filenames and directory names are case sensitive.</td>
</tr>
</tbody>
</table>
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 and then reconnect the switch power cord. After the switch performs POST, the switch begins the autoboot process. The boot loader prompts the user for a break key character during the boot-up sequence, as shown in this example:

```
***** The system will autoboot in 5 seconds *****
```

Send a break key to prevent autobooting.

The break key character is different for each operating system.

- On a SUN workstation running UNIX, Ctrl-C is the break key.
- On a PC running Windows 2000, Ctrl-Break is the break key.

Cisco TAC has tabulated break keys for most common operating systems and provided an alternative break key sequence for terminal emulators that do not support the break keys. To see that list go to: http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a0080174a34.shtml

When you enter the break key, the boot loader switch: prompt appears.

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 Cisco 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 Cisco IOS configuration file. For example, the name of the Cisco 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 Cisco 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>
<thead>
<tr>
<th>Variable</th>
<th>Boot Loader Command</th>
<th>Cisco 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 Cisco 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>Decides whether the switch automatically or manually boots. Valid values are 1, yes, 0, and no. If it is set to no or 0, the boot loader attempts to automatically boot the system. If it is set to anything else, you must manually boot the switch from the boot loader mode.</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 flash:filesystem:file-url boot loader 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 Cisco IOS uses to read and write a nonvolatile copy of the system configuration.</td>
<td>Specifies the filename that Cisco 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 1996 (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 1996 (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 find out 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 Cisco IOS Configuration Engine on the Cisco ME 3800X and 3600X switch.

Note


- 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 4-14

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 DeviceID 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.

**Figure 4-2 Initial Configuration Overview**
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 4-8
- Upgrading Devices with Cisco IOS Image Agent, page 4-13

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 4-1  Prerequisites for Enabling Automatic Configuration

<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>
<tr>
<td>DHCP server</td>
<td>• IP address assignment</td>
</tr>
<tr>
<td></td>
<td>• TFTP server IP address</td>
</tr>
<tr>
<td></td>
<td>• Path to bootstrap configuration file on the TFTP server</td>
</tr>
<tr>
<td></td>
<td>• Default gateway IP address</td>
</tr>
<tr>
<td>TFTP server</td>
<td>• A bootstrap configuration file that includes the CNS configuration commands that enable the switch to communicate with the Configuration Engine</td>
</tr>
<tr>
<td></td>
<td>• 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</td>
</tr>
<tr>
<td></td>
<td>• The CNS event agent configured to push the configuration file to the switch</td>
</tr>
<tr>
<td>CNS Configuration Engine</td>
<td>One or more templates for each type of device, with the ConfigID of the device mapped to the template.</td>
</tr>
</tbody>
</table>

**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>
</tbody>
</table>

**Step 2**

```
cns event {hostname | ip-address} [port-number] [backup] [failover-time seconds] [keepalive seconds retry-count] [reconnect time] [source ip-address]
```
Enable the event agent, and enter the gateway parameters.
- For `{hostname | ip-address}`, enter either the hostname or the IP address of the event gateway.
- (Optional) For `port number`, enter the port number for the event gateway. The default port number is 11011.
- (Optional) Enter `backup` to show that this is the backup gateway. (If omitted, this is the primary gateway.)
- (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.
- (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.
- (Optional) For `reconnect time`, enter the maximum time interval that the switch waits before trying to reconnect to the event gateway.
- (Optional) For `source ip-address`, enter the source IP address of this device.

**Note** Though visible in the command-line help string, the `encrypt` and the `clock-timeout time` keywords are not supported.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>end</th>
<th>Return to privileged EXEC mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>show cns event connections</td>
<td>Verify information about the event agent.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</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.
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></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>cns template connect name</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>cli config-text</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>cns connect name [retries number] [retry-interval seconds] [sleep seconds] [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></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>discover {controller controller-type</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>
### 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

Repeat Steps 7 to 8 to specify more interface parameters and CNS connect templates in the CNS connect profile.

### Step 10

**exit**

Return to global configuration mode.

### Step 11

**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

**cns interface num { dns-reverse | ipaddress | mac-address } [event] [image]**

(Optional) Set the unique EventID or ConfigID used by the Configuration Engine.

- 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.
Step 14

cns config initial {hostname \ ip-address} [port-number] [event] [no-persist] [page page] [source ip-address] [syntax-check]

Step 15

eend

Step 16

show cns config connections

Step 17

show running-config

---

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).

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)# 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 | hostname} [port-number] [source ip-address] Enable the configuration agent, and initiate a partial configuration.</td>
</tr>
<tr>
<td></td>
<td>• For {ip-address | hostname}, enter the IP address or the hostname of the configuration server.</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. The CNS image agent enables the managed device to initiate a network connection and request an image download allowing devices 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 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>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 host {ip-address} {hostname}</td>
<td>Enter the IP address and the hostname of the event gateway.</td>
</tr>
<tr>
<td>Step 3</td>
<td>cns trusted-server all-agents {hostname}</td>
<td>Specify a trusted server for CNS agent.</td>
</tr>
<tr>
<td>Step 4</td>
<td>no cns aaa enable cns event {ip-address} {port number}</td>
<td>Disable AAA authentication on the event gateway.</td>
</tr>
</tbody>
</table>
Displaying CNS Configuration

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

**Table 4-2 Displaying CNS Configuration**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show cns config connections</td>
<td>Displays the status of the CNS Cisco IOS agent connections.</td>
</tr>
<tr>
<td>show cns config outstanding</td>
<td>Displays information about incremental (partial) CNS configurations that have started but are not yet completed.</td>
</tr>
<tr>
<td>show cns config stats</td>
<td>Displays statistics about the Cisco IOS agent.</td>
</tr>
<tr>
<td>show cns event connections</td>
<td>Displays the status of the CNS event agent connections.</td>
</tr>
<tr>
<td>show cns event stats</td>
<td>Displays statistics about the CNS event agent.</td>
</tr>
<tr>
<td>show cns event subject</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 Cisco ME 3800X and 3600X switch.

- 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 5-30

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.

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

These sections contain 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:

- NTP
- 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 appears correctly 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.
Figure 5-1  Typical NTP Network Configuration

If the network is isolated from the Internet, Cisco’s implementation of NTP allows a device to act as if it is synchronized through NTP, when in fact it has learned 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 switch does not have a hardware-supported clock and cannot function as an NTP master clock to which peers synchronize themselves when an external NTP source is not available. The switch also has no hardware support for a calendar. As a result, the `ntp update-calendar` and the `ntp master` global configuration commands are not available.

- Default NTP Configuration, page 5-4
- Configuring NTP Authentication, page 5-4
- Configuring NTP Associations, page 5-5
- Configuring NTP Broadcast Service, page 5-6
• Configuring NTP Access Restrictions, page 5-8
• Configuring the Source IP Address for NTP Packets, page 5-10
• Displaying the NTP Configuration, page 5-11

Default NTP Configuration

Table 5-1 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 set 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</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>the key.</td>
</tr>
<tr>
<td></td>
<td>The switch does not synchronize to a device unless both have one</td>
</tr>
<tr>
<td></td>
<td>of these authentication keys, and the key number is specified by the</td>
</tr>
<tr>
<td></td>
<td>ntp trusted-key key-number command.</td>
</tr>
</tbody>
</table>
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>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 4. 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.

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>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 to send NTP broadcast packets, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 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>• (Optional) For number, specify the NTP version number. The range is 1 to 4. If you do not specify a version, Version 3 is used.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For keyid, specify the authentication key to use when sending packets to the peer.</td>
</tr>
<tr>
<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>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>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 gigabitethernet0/1
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>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 to receive NTP broadcast packets, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 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>Step 4 exit</td>
<td>Return to global configuration mode.</td>
</tr>
</tbody>
</table>
To disable an interface from receiving NTP broadcast packets, use the `no ntp broadcast client` interface configuration command. To change the estimated round-trip delay to the default, use the `no ntp broadcastdelay` global configuration command.

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

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

### Configuring NTP Access Restrictions

- Creating an Access Group and Assigning a Basic IP Access List, page 5-8
- Disabling NTP Services on a Specific Interface, page 5-10

### 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</td>
<td>configure terminal</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.
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>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 to disable.</td>
</tr>
<tr>
<td>ntp disable</td>
<td>Disable NTP packets from being received on the interface. By default, all interfaces receive NTP packets.</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 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>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>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 set by the outgoing interface.</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>

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`

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.

- Setting the System Clock, page 5-11
- Displaying the Time and Date Configuration, page 5-12
- 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>Step 1</td>
<td></td>
</tr>
<tr>
<td><code>clock set hh:mm:ss day month year</code> or <code>clock set hh:mm:ss month day year</code></td>
<td>Manually set the system clock using one of these formats.</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>

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>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>clock timezone zone hours-offset [minutes-offset]</code></td>
<td>Set the time zone. The switch keeps internal time in universal time coordinated (UTC), so this command is used only for display purposes and when the time is manually set.</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>

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>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>clock summer-time zone recurring [week day month hh:mm week day month hh:mm [offset]]</td>
<td>Configure summer time to start and end on the specified days every year. Summer time is disabled by default. If you specify clock summer-time zone recurring without parameters, the summer time rules default to the United States rules.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For zone, specify the name of the time zone (for example, PDT) to be displayed when summer time is in effect.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For week, specify the week of the month (1 to 5 or last).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For day, specify the day of the week (Sunday, Monday...).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For month, specify the month (January, February...).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For hh:mm, specify the time (24-hour format) in hours and minutes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For offset, specify the number of minutes to add during summer time. The default is 60.</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>

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>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>clock summer-time zone date [month date year hh:mm month date year hh:mm [offset]]</td>
</tr>
<tr>
<td>or</td>
<td>clock summer-time zone date [date month year hh:mm date month year hh:mm [offset]]</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.

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

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

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

## Configuring a System Name and Prompt

You configure the system name on the 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.

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*.

- 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 <em>name</em></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 File Transfer Protocol (FTP) system is identified as *ftp.cisco.com*.

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

These sections contain 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  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>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 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 Dynamic Host Configuration Protocol (DHCP) server, then the default domain name might be set by the BOOTP or DHCP server (if the servers were configured with this information).</td>
</tr>
<tr>
<td>Step 3 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>Step 4 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>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>
If you use the switch IP address as its hostname, the IP address is used and no DNS query occurs. If you configure a hostname that contains no periods (.), a period followed by the default domain name is appended to the hostname before the DNS query is made to map the name to an IP address. The default domain name is the value set by the `ip domain-name` global configuration command. If there is a period (.) in the hostname, the Cisco IOS software looks up the IP address without appending any default domain name to the hostname.

To remove a domain name, use the `no ip domain-name name` global configuration command. To remove a name server address, use the `no ip name-server server-address` global configuration command. To disable DNS on the switch, use the `no ip domain-lookup` global configuration command.

### Displaying the DNS Configuration

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

### Creating a Banner

You can configure a message-of-the-day (MOTD) and a login banner. The MOTD banner 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 appears after the MOTD banner and before the login prompts.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
</table>

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

- 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.
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>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 banner motd c message c</td>
<td>Specify the message of the day.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>For message, enter a banner message up to 255 characters. You cannot use the delimiting character in the message.</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 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.
#
Switch(config)#
```

This example shows the banner that appears 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>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: banner login (c) message (c)</td>
<td>Specify the login message.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>For message, enter a login message up to 255 characters. You cannot use the delimiting character in the message.</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 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, page 5-20
- MAC Addresses and VLANs, page 5-20
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 be forwarded to port 1 in VLAN 1 and ports 1, 9, and 10 in VLAN 5.

Each VLAN maintains its own logical address table. A known address in one VLAN is unknown in another until it is learned or statically associated with a port in the other VLAN.

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 5-28 for more information.
## Default MAC Address Table Configuration

### Table 5-3  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>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 mac address-table aging-time [0</td>
<td>10-1000000] [vlan vlan-id]</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show mac address-table aging-time</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 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>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 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 change</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>mac address-table notification change</code></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 gigabitethernet0/2
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.

---

**Command** | **Purpose**
--- | ---
**Step 5** | _mac address-table notification change [interval value] [history-size value]_ Enter the trap interval time and the history table size.
- (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.
- (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.
**Step 6** | _interface interface-id_ Enter interface configuration mode, and specify the interface on which to enable the SNMP MAC address notification trap.
**Step 7** | _snmp trap mac-notification change {added | removed}_ Enable the MAC address change notification trap on the interface.
- Enable the trap when a MAC address is _added_ on this interface.
- Enable the trap when a MAC address is _removed_ from this interface.
**Step 8** | _end_ Return to privileged EXEC mode.
**Step 9** | _show mac address-table notification change interface show running-config_ Verify your entries.
**Step 10** | _copy running-config startup-config_ (Optional) Save your entries in the configuration file.
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>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 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>snmp-server enable traps mac-notification move</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>mac address-table notification mac-move</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show mac address-table notification mac-move</td>
</tr>
<tr>
<td>show running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable MAC address-move notification traps, use the no snmp-server enable traps mac-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>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</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>Step 3</td>
<td>snmp-server enable traps mac-notification threshold</td>
</tr>
<tr>
<td>Step 4</td>
<td>mac address-table notification threshold</td>
</tr>
<tr>
<td>Step 5</td>
<td>mac address-table notification threshold [limit percentage]</td>
</tr>
<tr>
<td></td>
<td>[interval time]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
</tr>
<tr>
<td>Step 7</td>
<td>show mac address-table notification threshold</td>
</tr>
<tr>
<td></td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 8</td>
<td>copy running-config startup-config</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 or multicast 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 defines 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. You can specify a different list of destination ports for each source port.

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.
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>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>mac address-table static mac-addr vlan vlan-id interface interface-id</td>
</tr>
<tr>
<td></td>
<td>• For mac-addr, 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 vlan-id, specify the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094; do not enter leading zeros.</td>
</tr>
<tr>
<td></td>
<td>• For interface-id, specify the interface to which the received packet is forwarded. Valid interfaces include physical ports or port channels. For static multicast addresses, you can enter multiple interface IDs. For static unicast addresses, you can enter only one interface at a time, but you can enter the command multiple times with the same MAC address and VLAN ID.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show mac address-table static</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</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 port:

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet0/1
```

### 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.
Managing the MAC Address Table

- 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><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>mac address-table static mac-addr vlan vlan-id drop</code></td>
</tr>
<tr>
<td></td>
<td>- For <code>mac-addr</code>, specify a source or destination unicast MAC address. Packets with this MAC address are dropped.</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. Valid VLAN IDs are 1 to 4094.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show mac address-table static</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>copy running-config startup-config</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:

- You can disable MAC address learning on a VLAN or on an Ethernet flow point (EFP) service-instance bridge domain.
- Disable MAC address learning on a VLAN or bridge domain by entering the `no mac address-table learning {vlan vlan-id | bridge-domain domain-id}` command.
- 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.
- 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.

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

<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 mac address-table learning {vlan vlan-id</td>
<td>Disable MAC address learning on the specified VLAN or bridge domain.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>4</td>
<td>show mac address-table learning [vlan vlan-id]</td>
<td>Verify the configuration.</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 reenable MAC address learning on a VLAN or bridge, use the `default mac address-table learning {vlan vlan-id | bridge-domain domain-id}` global configuration command. You can also reenable MAC address learning on a VLAN by entering the `mac address-table learning {vlan vlan-id | bridge-domain domain-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` command. The second command causes the configuration to appear in 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` 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 ip igmp snooping groups</td>
<td>Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.</td>
</tr>
<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>
</tbody>
</table>
Managing the ARP Table

To communicate with a device (over Ethernet, for example), the software first must learn the 48-bit MAC address or the local data link address of that device. The process of learning 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. Using an IP address, ARP finds the associated MAC address. When a MAC address is found, 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 arp keyword) is enabled on the IP interface.

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

For CLI procedures, see the Cisco IOS Release 12.2 documentation on Cisco.com.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mac address-table count</td>
<td>Displays the number of addresses present in all VLANs or the specified VLAN.</td>
</tr>
<tr>
<td>show mac address-table dynamic</td>
<td>Displays only dynamic MAC address table entries.</td>
</tr>
<tr>
<td>show mac address-table interface</td>
<td>Displays the MAC address table information for the specified interface.</td>
</tr>
<tr>
<td>show mac address-table learning</td>
<td>Displays MAC address learning status of all VLANs or the specified VLAN.</td>
</tr>
<tr>
<td>show mac address-table notification</td>
<td>Displays the MAC notification parameters and history table.</td>
</tr>
<tr>
<td>show mac address-table static</td>
<td>Displays only static MAC address table entries.</td>
</tr>
<tr>
<td>show mac address-table vlan</td>
<td>Displays the MAC address table information for the specified VLAN.</td>
</tr>
</tbody>
</table>
Configuring Synchronous Ethernet

The ME 3800X and ME 3600X switches support Synchronous Ethernet (SyncE), which is the PHY-layer frequency-synchronization solution for IEEE 802.3 links. It is an evolution of the conventional Ethernet and Ethernet + SDH and SONET-based synchronization. SyncE is used to synchronize and send clock information to remote sites on the network. Each network element along the synchronization path must support SyncE. SyncE provides only frequency synchronization, not related to time or space.

- Understanding SyncE, page 6-1
- Configuring SyncE, page 6-9
- Monitoring SyncE, page 6-13

Understanding SyncE

SyncE provides a method to synchronize the Ethernet network by having all Ethernet ports send data based on a reference clock. All devices supporting SyncE must send and receive data in cycles of fixed size and duration. The data size depends on the Ethernet speed. The rate of transmission is 8000 cycles per second. Each device must be able to support a system timing master, which is the synchronization source. A sync port is the port on which synchronization information is received. All SyncE frames coming from the sync port are the source of synchronization for all other ports on the device.

The switch 10 Gigabit Ethernet uplink ports or BITS interface support line clock recovery, sending and receiving clock information. Downlink ports do not perform clock recovery and can only send clock signals.

The switch supports TI (1544 kilobits/s) and E1 (2048 kb/s or 2048 KHz) clock timing synchronization.

- Reference Clocks, page 6-1
- BITS Interface, page 6-2
- Synchronous Ethernet and Ethernet Synchronization Messaging Channel, page 6-3

Reference Clocks

A switch comes up in a free-run state, using the internal oscillator (Stratum 3) for synchronization. If there is a valid clock reference with a set priority, the switch locks to that reference. If there is no reliable clock source available, the switch remains in free-run mode. If the current clock becomes invalid, the switch goes into holdover mode and replays the saved clock from the last source. The switch SyncE LEDs show the status of the internal clock: locked (green), free run (off), or in a holdover state (amber).
The reference clock source can be:

- A Building Integrated Timing Supply (BITS) clock input
- A PHY-recovered clock from uplink ports. The ME 3800X and 3600X switch supports a PHY-recovered clock only from the small form-factor pluggable (SFP+) uplink ports with 10 Gigabit SFP+ or 1000BASE-X fiber SFP modules.

All uplink and downlink ports transmit data on the same reference clock.

The switch monitors each input clock for frequency accuracy and activity. An input clock with a frequency out-of-band alarm or an activity alarm is invalid. Invalid clocks are not selected as the reference clock.

During normal operation, the reference clock is selected based on an algorithm that uses the priority rankings that you assign to the input clocks by using the `network-clock input-source priority` global configuration command. Priority 1 is the highest, and priority 15 is the lowest. If you try to assign the same priority to more than one clock, an error message appears. Unused input clocks are given a priority value of 0, which disables the clocks and makes them unavailable for selection. The clock selection is based on signal failure, priority, and manual configuration. If you have not manually configured a reference clock, the algorithm selects the clock with the highest priority that does not experience signal failure.

With this configuration, pure priority-based mode, an intermittent failure or changes in the network topology can cause timing loops or a loss of connectivity with the clock reference. The Ethernet Synchronous Messaging Channel (ESMC) with Synchronization Status Messages (SSM) provides a way to implement quality in synchronous networks.

Reference clocks operate in revertive or nonrevertive mode, configured by using the `network-clock revertive` global configuration command. The revertive clocks will be in non-revertive mode by default.

- In revertive mode, if an input clock with a higher priority than the selected reference becomes available, the higher priority reference is immediately selected.
- In nonrevertive mode, if a new input clock with a higher priority becomes available, the higher-priority clock is selected. This means, among all available input reference clocks, the higher-priority clock is selected.
- In non revertive mode, when an input clock with a high priority present on the system becomes invalid or unavailable, a lower priority clock will be selected. However when the higher priority clock becomes available again it will not be selected.

**Note**

In revertive mode of operation, when the lost high priority reference becomes available again, it is selected. However, in non-revertive mode of operation, the regained high priority reference is not selected.

You can use the `network-clock switch` privileged EXEC command to configure the input reference to be either forced or automatically selected by the selection algorithm based on the highest priority valid input clock. In revertive mode, the forced clock automatically becomes the selected reference. In nonrevertive mode, the forced clock becomes the selected reference only when the existing reference is invalidated or unavailable.

### BITS Interface

The ME 3800X and ME 3600X switch supports a BITS interface through an RJ-45 connector. The connection can be used for sending and receiving T1 and E1 timing signals.
You can configure all Ethernet ports to send data referenced to the BITS recovered clock. The BITS signal is used as long as it does not have these faults:

- loss of signal
- out of frame
- alarm-indication signal
- remote alarm indication

The switch supports BITS IN and BITS OUT, and recovers and sends BITS timing, T1, E1. The switch does not support T1 or E1 data transmission. You can configure the BITS interface input and output, including line coding and line buildout (output). You can also shut down the BITS controller.

The switch supports these BITS configurations:

- E1 Mode:
  - 2048 KHz
  - Framing mode: FAS, MFAS, FASCRC4, MFASCRC4 with line coding: AMI, HDB3
- T1 Mode:
  - Framing mode: D4 and ESF
  - Line coding: AMI, B8ZS
  - Line buildout (output): 0 to 133 feet, 133 to 266 feet, 266 to 399 feet, 399 to 533 feet, or 533 to 655 feet

**Synchronous Ethernet and Ethernet Synchronization Messaging Channel**

The ME3600/ME3800 switches support the following Synchronous Ethernet (SyncE) and Ethernet Synchronization Messaging Channel (ESMC) features:

- Common IOS CLI configuration
- Configuration on all ports, including BITS ports and copper ports
- Can be enabled or disabled on individual ports
- Synchronous Ethernet clock derived from user configuration
- Synchronous Status Message (SSM) on BITS interface
- Ethernet Synchronous Messaging Channel (ESMC) on all Ethernet ports

Clock selection is configured by the user based on clock priority and ESMC/SSM messages received from all sources and ports.

A Synchronous Status Message (SSM) informs the peer about the quality of the local clock source and is used to detect and avoid timing loops. SSMS are transported over the Ethernet Synchronization Messaging Channel (ESMC). All SSM information transported over Ethernet ports must be in the ESMC message format (G.8264).

The BITS port can be configured as a T1 or E1 interface.

- For T1s, SSM messages are transported over the 4 Kbps datalink channel.
- For E1s, SSM messages are transported over the E1 signaling channel.
Configuring Synchronous Ethernet

To configure synchronous ethernet in Release 15.1(2)EY

1. Replace existing syncE configurations with the new configurations given in the “Configuring Synchronous Ethernet” section.
2. Copy the changed configuration to startup-config
3. Reload the switch with the 15.1(2)EY image.

Restrictions
T1 mode supports only D4 and ESF framing.

Configuring Synchronous Ethernet

The following sections show the old and new methods of configuring synchronous ethernet on the ME3600/ME3800 switches:

- Configuring Input Clock and Priority
- Configuring Hold-off timer
- Configuring Hold-over Timer
- Configuring Wait-to-Restore Timer
- Configuring Revertive Mode
- Configuring EEC Option
- Configuring BITS
- Configuring BITS Input
- Configuring BITS Output
- Configuring Output Clock
- SyncE Show Commands

Configuring Input Clock and Priority

Old Configuration

Switch(config)# network-clock_select 2 ?
  BITS  BITS port clock
  SYNCE  Sync Ethernet

Switch(config)# network-clock_select 2 SYNCE ?
  <0-1>  port

New Configuration

Switch(config)# network-clock input-source ?
  <1-250>  Priority
Switch(config)# network-clock input-source 1 ?
  external  External Interface (BITS/SSU/GPS)
  interface  Specify Ethernet, Sonet or ToP Interface

SynChE as Clock Source Example Configuration

Switch(config)# network-clock input-source 1 interface tenGigabitEthernet ?
Configuring Synchronous Ethernet

BITS as Clock Source Example Configuration

Switch(config)# network-clock input-source 1 external 1/0/0 e1 ?
  cas   E1 Channel Associated Signal Mode
  crc4  E1 With CRC4 Signal Mode
  fas   E1 Frame Alignment Signal Mode

Note
Currently, the E1 and T1 modes cannot be configured independently.

The default values for the E1 mode are as follows:

- Framing: FAS
- Line coding: AMI

The default values for the T1 mode are as follows:

- Framing: D4
- Line coding: AMI
- Line build out: 0-133ft

Configuring Hold-off timer

Old Configuration
Switch(config)# network-clock_select hold-off-timeout ?
  <50-10000>  holdoff-val in ms, default 300 ms

New Configuration
Switch(config)# network-clock hold-off ?
  0           holdoff disable
  <50-10000>  msec (default 300 msecs)

Configuring Hold-over Timer

Old Configuration
Switch(config)# network-clock_select hold-timeout ?
  <0-86400>  hold-timeout-val
  infinite   Infinite hold-over.

New Configuration
CLI is not available.

Configuring Wait-to-Restore Timer

Old Configuration
Switch(config)# network-clock_select wait-to-restore-timeout ?
  <0-720>  wtr-val in seconds, default 300 seconds
New Configuration
Switch(config)# network-clock wait-to-restore ?
<0-86400> sec (default 300 seconds)

Configuring Revertive Mode

Old Configuration
Switch(config)# network-clock_select mode ?
   nonrevert  Specify non revertive mode.
   revert    Specify revertive mode.

New Configuration
Switch(config)# network-clock revertive
Switch(config)# no network-clock revertive

Configuring EEC Option

Old Configuration
Switch(config)# network-clock_select option ?
   option1  EEC Option 1.
   option2  EEC Option 2.

New Configuration
Switch(config)# network-clock synchronization ssm option ?
   1  Synchronization networking Option I
   2  Synchronization networking Option II
Switch(config)# network-clock synchronization ssm option 2 ?
   GEN1  Option II Generation 1
   GEN2  Option II Generation 2

Configuring BITS

Old Configuration
Switch(config)# controller BITS ?
   input      Configure BITS INPUT
   output     Configure BITS OUTPUT
   shutdown   Shut down BITS controller

New Configuration
Switch(config)# controller BITS ?
   input      Configure BITS input
   output     Configure BITS output
   shutdown   Shut down BITS controller
Configuring BITS Input

**Old Configuration**

controller BITS input applique ?
  E1 Link type E1
  T1 Link type T1

Switch(config)# controller BITS input applique E1 ?
  2048KHz  2048 KHz clock interface
  framing BITS framing options for E1

Switch(config)# controller BITS input applique E1 framing ?
  fas_crc4  FASCRC4
  fas_nocrc  FAS
  mfas_crc4  MFASCRC4
  mfas_nocrc  MFAS

Switch(config)# controller BITS input applique E1 framing fas_crc4 linecode ?
  ami  AMI encoding
  hdb3  HD83 encoding

**New Configuration**

Same as Old Configuration.

Configuring BITS Output

**Old Configuration**

Switch(config)# controller BITS output applique ?
  E1 Link type E1
  T1 Link type T1

Switch(config)# controller BITS output applique T1 framing ?
  d4  D4
  esf  Extended Superframe

Switch(config)# controller BITS output applique T1 framing d4 linecode ?
  ami  AMI encoding
  b8zs  B8ZS encoding

Switch(config)# controller BITS output applique T1 framing d4 linecode ami line-build-out ?

  0-133ft  0 ft to 133 ft
  133-266ft  133 ft to 266 ft
  266-399ft  266 ft to 399 ft
  399-533ft  399 ft to 533 ft
  533-655ft  533 ft to 655 ft

**New Configuration**

Same as Old Configuration.
The controller BITS CLIs should be used to configure shutdown, linecode and line-build-out as these options are missing in netsync PI infrastructure CLIs. Once the netsync infrastructure CLIs implement these configuration options, the platform "controller BITS" CLIs will be deprecated.

**Configuring Output Clock**

**Old Configuration**

Switch(config)# network-clock_select output ?
  <1-23> priority
  output Configure BITS OUT (T4 = T0)

Switch(config)# network-clock_select output 2 SYNCE ?
  <0-1> port

**New Configuration**

Switch(config)# network-clock output-source ?
  line Line Input
  system System clock (T0)

**Tengig Clock for BITS OUT Example Configuration**

Switch(config)# network-clock output-source line ?
  <1-250> Priority
Switch(config)# & network-clock output-source line 10 interface tenGigabitEthernet ?
  <0-0> TenGigabitEthernet interface number

**System Clock for BITS OUT Example Configuration**

Switch(config)# network-clock output-source system ?
  <1-250> Priority
Switch(config)# network-clock output-source system 10 external 1/0/0 ?
  t1 T1 signal mode output

**SyncE Show Commands**

The following example shows how to display the SyncE network-clock information:

Switch# show network-clock synchronization ?
  detail Detail
  external External Interface (BITS/SSU/GPS)
  global Display global parameters
  interface Specify Ethernet or Sonet Interface
  runtime Runtime Information
  | Output modifiers

Switch# show network-clock synchronization detail

**SyncE Debug Commands**

The following example shows the network-clock (PI) debug command:

RB#debug network-clock ?
Configuring SyncE

SyncE limitations on copper ports:

- To receive clock data from an ME 3600X-TS 1 Gigabit Ethernet copper SFP interface, the link partner must not be the 802.3 master port when 802.3 Clause 28 autonegotiation completes.
- On ME3600X-FS or ME3800X switches, SyncE is not supported on 1 Gigabit Ethernet copper SFPs for the first release.
- Default SyncE Configuration, page 6-9
- Configuring the Network Clock Selection, page 6-9
- Configuring the BITS Interface, page 6-10
- Selecting the Network Clock, page 6-12
- Configuring SyncE using ESMC and SSM, page 6-12

Default SyncE Configuration

Synchronous Ethernet can only be configured on 10 Gigabit Ethernet interfaces.
1 Gigabit Ethernet interfaces transmit SyncE with no configuration required. No configuration is needed to send clock timing in uplink or downlink interfaces.

Configuring the Network Clock Selection

Beginning in privileged EXEC mode, follow these steps to configure the SyncE network clock.

<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>network-clock input-source priority [external] [interface]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 6  Configuring Synchronous Ethernet

**Configuring SyncE**

Enter the `no network-clock priority` or `network-clock output-source` to remove the selected priority. Enter the `no network-clock revertive` to select the other mode.

This example configures the BITS clock with a priority of 2 and the SyncE input port as 10 Gigabit Ethernet port 0/1 with the switching mode as nonrevertive.

```
Switch (config)# network-clock input-source 2 external 1/0/0 e1
Switch (config)# network-clock input-source 1 interface tenGigabitEthernet
Switch (config)# network-clock revertive
Switch (config)# end
```

### Configuring the BITS Interface

Beginning in privileged EXEC mode, follow these steps to configure the BITS interface. The Ethernet Equipment Clock (EEC) mode of operation is based on the area of deployment.

<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>network-clock synchronization ssm option {option1</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 6 Configuring Synchronous Ethernet

Configuring SyncE

### Step 3

controller BITS input applique E1 {2048KHz | framing option linecode {ami | hdb3}}

or

controller BITS input applique T1 framing {d4 | esf} linecode {ami | b8zs}

(Optional) Configure the controller BITS input framing and coding options.

For E1 input:
- **2048KHz**—Select 2048 KHz input.
- **framing option**—Select one of these options:
  - fas_crc4—FASCRC4
  - fas_nocrc—FAS
  - mfas_crc4—MFASCRC4
  - mfas_nocrc—MFAS

For T1 input:
- **d4 linecode**—D4
- **esf linecode**—Extended superframe
- **linecode ami**—AMI encoding
- **linecode b8zs**—B8ZS encoding

### Step 4

controller BITS output applique E1 {2048KHz | framing options} linecode {ami | hdb3}

or

controller BITS output applique T1 framing {d4 | esf} linecode {ami | b8zs} line-build-out length

(Optional) Configure the controller BITS output framing and coding options.

For E1 output:
- **2048KHz**—Select 2048 KHz input.
- **framing**—Select one of these options:
  - fas_crc4—FASCRC4
  - fas_nocrc—FAS
  - mfas_crc4—MFASCRC4
  - mfas_nocrc—MFAS

For T1 framing output:
- **d4 linecode**—D4
- **esf linecode**—Extended superframe
- **linecode ami**—AMI encoding
- **linecode b8zs**—B8ZS encoding
- **line-build-out length**—Select a line length:
  - 0-133ft
  - 133-266ft
  - 266-399ft
  - 399-533ft
  - 533-655ft

### Step 5

controller BITS shutdown

Shut down the BITS controller.

### Step 6

end

Return to privileged EXEC mode.
### Configuring SyncE

**Enter the** `no network-clock synchronization ssm option option1` **or the** `network-clock synchronization ssm option option2` **to select the other option, mode with the default E1 or T1 values.**

Use the `no` form of each command to remove the configuration or return to the default.

This example configures EEC as T1 with ESF framing, B8ZS line coding, and 1 to 133 foot line buildout.

```
Switch (config)# network-clock synchronization ssm option option2
Switch (config)# controller BITS input applique T1 framing esf linecode b8zs
Switch (config)# controller BITS output applique T1 framing esf linecode b8zs
Switch (config)# line-build0-out 0-133ft
Switch (config)# end
```

**Applique type is T1**

*Line Coding is B8ZS(Rx), B8ZS(Tx)*

*Framing is ESF(Rx), ESF(Tx)*

*Line Build Out is 0-133ft*

*No alarms detected.*

### Selecting the Network Clock

You can force selection of a particular network clock or select automatic clock selection where the switch uses the selection algorithm based on the priority and the validity of the input.

Beginning in privileged EXEC mode, use this step to set the SyncE network clock.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>`network-clock {clear</td>
</tr>
<tr>
<td></td>
<td>Select one of these options:</td>
</tr>
<tr>
<td></td>
<td>• <code>clear</code>—Use to clear network clock synchronization</td>
</tr>
<tr>
<td></td>
<td>• <code>set</code>—Set network clock synchronization</td>
</tr>
<tr>
<td></td>
<td>• <code>switch</code>—Switch selected synchronization source.</td>
</tr>
<tr>
<td>If the switch is in nonrevertive mode, the clock input does not change unless the current clock becomes invalid.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>show network-clocks</code></td>
</tr>
<tr>
<td></td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>copy running-config startup config</code></td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the switch startup configuration file.</td>
</tr>
</tbody>
</table>

### Configuring SyncE using ESMC and SSM
To enable ESMC process use the following steps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enter privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 3 esmc process</td>
<td>Enables ESMC process.</td>
</tr>
</tbody>
</table>

To configure the interface to send or receive a particular clock use the following steps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enter privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 3 interface interface-id</td>
<td>Enter the interface ID, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 4 network-clock source quality-level value {tx</td>
<td>rx}</td>
</tr>
</tbody>
</table>

To configure BITS port to send or receive a particular-clock use the following steps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enter privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 3 network-clock quality-level {tx</td>
<td>rx}value external port/slot</td>
</tr>
</tbody>
</table>

## Monitoring SyncE

Use these privileged EXEC commands to view SyncE configuration on a switch:

- **show controller BITS**
  
  ```
  Switch# show controller BITS
  
  Appliance type is T1
  Line Coding is B8ZS(Rx), B8ZS(Tx)
  Framing is ESF(Rx), ESF(Tx)
  Line Build Out is 0-133ft
  No alarms detected.
  ```

- **show network-clock synchronization**
  
  ```
  Switch# show network-clock synchronization detail
  
  Symbols: En - Enable, Dis - Disable, Adis - Admin Disable
  ```
NA - Not Applicable
* - Synchronization source selected
# - Synchronization source force selected
& - Synchronization source manually switched

Automatic selection process: Enable
Equipment Clock: 1544 (EEC-Option2)
Clock Mode: QL-Enable
ESMC: Enabled
SSM Option: GEN1
T0: TenGigabitEthernet0/2
Hold-off (global): 300 ms
Wait-to-restore (global): 300 sec
Tsm Delay: 180 ms
Revertive: No
Force Switch: FALSE
Manual Switch: FALSE
Number of synchronization sources: 2
Squelch Threshold: QL-ST3
sm(netsync NETCLK_QL_ENABLE), running yes, state 1A
Last transition recorded: (ql_mode_enable)-> 1A (begin)-> 1A (src_added)-> 1A (src_added)-> 1A (ql_change)-> 1A (ql_change)-> 1A (set_lo)-> 1A (clear_lo)-> 1A

Nominated Interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>SigType</th>
<th>Mode/QL</th>
<th>Prio</th>
<th>QL_IN</th>
<th>ESMC Tx</th>
<th>ESMC Rx</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal</td>
<td>NA</td>
<td>NA/Dis</td>
<td>251</td>
<td>QL-ST3</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Te0/1</td>
<td>NA</td>
<td>Sync/En</td>
<td>1</td>
<td>QL-FAILED</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>*Te0/2</td>
<td>NA</td>
<td>Sync/En</td>
<td>2</td>
<td>QL-PRS</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

T4 Out

External Interface | SigType     | Input         | Prio | Squelch | AIS  |
External 1/0/0     | T1 ESF      | Internal      | 2    | FALSE   | FALSE |

Interface:
-----------------------------
Local Interface: Internal
Signal Type: NA
Mode: NA(Ql-enabled)
SSM Tx: DISABLED
SSM Rx: DISABLED
Priority: 251
QL Receive: QL-ST3
QL Receive Configured: -
QL Receive Overrided: -
QL Transmit: -
QL Transmit Configured: -
Hold-off: 0
Wait-to-restore: 300
Lock Out: FALSE
Signal Fail: FALSE
Alarms: FALSE
Slot Disabled: FALSE
SNMP input source index: 1
SNMP parent list index: 0

Local Interface: Te0/1
Signal Type: NA
Mode: Synchronous(Ql-enabled)
ESMC Tx: ENABLED
ESMC Rx: ENABLED
Priority: 1
QL Receive: QL-DUS
QL Receive Configured: -
QL Receive Overrided: QL-FAILED
QL Transmit: -
QL Transmit Configured: -
Hold-off: 300
Wait-to-restore: 300
Lock Out: FALSE
Signal Fail: TRUE
Alarms: FALSE
Slot Disabled: FALSE
SNMP input source index: 2
SNMP parent list index: 0

Local Interface: Te0/2
Signal Type: NA
Mode: Synchronous(QL-enabled)
ESMC Tx: ENABLED
ESMC Rx: ENABLED
Priority: 2
QL Receive: QL-PRS
QL Receive Configured: -
QL Receive Overrided: -
QL Transmit: QL-DUS
QL Transmit Configured: -
Hold-off: 300
Wait-to-restore: 20
Lock Out: FALSE
Signal Fail: FALSE
Alarms: FALSE
Slot Disabled: FALSE
SNMP input source index: 3
SNMP parent list index: 0

External 1/0/0 t1 esf's Input:
Internal
Local Interface: Internal
Signal Type: NA
Mode: NA(QL-enabled)
SSM Tx: DISABLED
SSM Rx: DISABLED
Priority: 2
QL Receive: QL-ST3
QL Receive Configured: -
QL Receive Overrided: -
QL Transmit: -
QL Transmit Configured: -
Hold-off: 300
Wait-to-restore: 300
Lock Out: FALSE
Signal Fail: FALSE
Alarms: FALSE
Slot Disabled: FALSE
SNMP input source index: 1
SNMP parent list index: 1

- show esmc

Switch# show esmc

Interface: GigabitEthernet0/0/0
Administrative configurations:
  Mode: Synchronous
  ESMC TX: Enable
ESMC RX : Enable
QL RX configured : NA
QL TX configured : NA
Operational status:
   Port status: UP
   QL Receive: QL-SSU-B
ESMC Information rate : 1 packet/second
ESMC Expiry: 5 second
Configuring the Switch External Alarms

On the ME 3800X and ME 3600X switch, you can configure external alarm inputs.

Understanding Switch Alarms

You can connect up to four alarm inputs from external devices in your environment, such as a door, a temperature gauge, or a fire alarm, to the alarm input port on the switch front panel. Figure 7-1 shows the location of the alarm pinouts.

For each alarm input, you can configure an open or closed circuit to trigger an alarm and configure the severity of the alarm. A triggered alarm generates a system message. If you enter a descriptive name for the alarm, that name is included in the system message. A triggered alarm also turns on the LED display (the LED is normally off, meaning no alarm). See the Cisco ME-3800X and ME 3600X Hardware Installation Guide for information about the LEDs.

The alarm trigger setting is **open** or **closed**. If not set, the alarm is triggered when the circuit closes.

- Open means that the normal condition has current flowing through the contact (normally closed contact). The alarm is generated when the current stops flowing.
- Closed means that no current flows through the contact (normally open contact). The alarm is generated when current does flow.
You can set the alarm severity to **minor**, **major**, or **critical**. The severity is included in the alarm message and also sets the LED color when the alarm is triggered. The LED is amber for a minor alarm, red for a major alarm, and blinking red for a critical alarm. If not set, the default alarm severity is **minor**.

## Configuring Switch Alarms

Beginning in privileged EXEC mode, follow these steps to configure alarm contacts.

<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>alarm-contact contact-number description string</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>alarm-contact {contact-number</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 env alarm-contact</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To delete the alarm description, enter the **no alarm-contact contact-number description** privileged EXEC command. To set the alarm severity to **minor** (the default), enter the **no alarm-contact {contact-number | all} severity**. To set the alarm contact trigger to **closed** (the default), enter the **no alarm-contact {contact-number | all} trigger**.

To see the alarm configuration and status, enter the **show env alarm-contact** privileged EXEC command.

For more detailed information about the alarm commands, see the command reference for this release.

**Note** The switch supports the CISCO-ENTITY-ALARM-MIB for these alarms.
This example configures alarm input 2 named *door sensor* to assert a major alarm when the door circuit is closed and then displays the status and configuration for all alarms:

```
Switch(config)# alarm-contact 2 description door sensor
Switch(config)# alarm-contact 2 severity major
Switch(config)# alarm-contact 2 trigger closed
Switch(config)# end
Switch(config)# show env alarm-contact
Switch# show env alarm-contact
ALARM CONTACT 1
  Status: not asserted
  Description: test_1
  Severity: critical
  Trigger: open
ALARM CONTACT 2
  Status: not asserted
  Description: door sensor
  Severity: major
  Trigger: closed
ALARM CONTACT 3
  Status: not asserted
  Description: flood sensor
  Severity: critical
  Trigger: closed
ALARM CONTACT 4
  Status: not asserted
  Description: 
  Severity: critical
  Trigger: closed
```
CHAPTER 8

Configuring SDM Templates

This chapter describes how to configure the Switch Database Management (SDM) templates on the Cisco Metro Ethernet (ME) 3600X and 3800X switch.

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

- Understanding the SDM Templates, page 8-1
- Configuring the Switch SDM Template, page 8-3
- Displaying the SDM Templates, page 8-4

Understanding the SDM Templates

The Switch Database Management (SDM) templates are used to optimize system resources in the switch to support specific features, depending on how the switch is used in the network. The SDM templates allocate TCAM resources to support different features. You can use the SDM templates to optimize resources for different features. You can select the default template to balance system resources or select specific templates to support features such as only IPv4 or only IPv6 in the hardware.

Only three licenses support SDM templates, Metro IP Access, Advanced Metro IP Access, and Scaled Metro Aggregation Services. Use the help option of the `sdm prefer` command to display the templates supported under each license.

Table 8-1 shows the approximate number of each resource supported in each of the templates for a switch running the metro IP access image.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default</th>
<th>IPv4 SDM template</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC table</td>
<td>8 K</td>
<td>8 K</td>
</tr>
<tr>
<td>IPv4 routes</td>
<td>20</td>
<td>24 K</td>
</tr>
<tr>
<td>IPv6 routes</td>
<td>5 K</td>
<td>4 K</td>
</tr>
<tr>
<td>IPv4 routing groups</td>
<td>1 K</td>
<td>1 K</td>
</tr>
<tr>
<td>Multicast Groups</td>
<td>1 K</td>
<td>1 K</td>
</tr>
</tbody>
</table>
Table 8-1  
**Approximate Number of Feature Resources Allowed by Each Template (continued)**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default</th>
<th>IPv4 SDM template</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge Domains</td>
<td>4 K</td>
<td>4 K</td>
</tr>
<tr>
<td>Ethernet Flow Point (EFP)</td>
<td>4 K</td>
<td>4 K</td>
</tr>
<tr>
<td>ACL entries</td>
<td>2 K</td>
<td>2 K</td>
</tr>
<tr>
<td>IPv4 QoS classification</td>
<td>4 K</td>
<td>4 K</td>
</tr>
</tbody>
</table>

Table 8-2 shows the approximate number of each resource supported in each of the templates for a switch running the advanced metro IP access image.

Table 8-2  
**Approximate Number of Feature Resources Allowed by Each Template**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default</th>
<th>Advanced Metro IP Access IP SDM template</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC table</td>
<td>16 K</td>
<td>16 K</td>
</tr>
<tr>
<td>IPv4 Routes</td>
<td>20</td>
<td>24 K</td>
</tr>
<tr>
<td>IPv6 Routes</td>
<td>5 K</td>
<td>3 K</td>
</tr>
<tr>
<td>IPv4 Routing Groups</td>
<td>1 K</td>
<td>1 K</td>
</tr>
<tr>
<td>Multicast Groups</td>
<td>1 K</td>
<td>1 K</td>
</tr>
<tr>
<td>Bridge Domains</td>
<td>4 K</td>
<td>4 K</td>
</tr>
<tr>
<td>Ethernet Flow Point (EFP)</td>
<td>4 K</td>
<td>4 K</td>
</tr>
<tr>
<td>ACL entries</td>
<td>2 K</td>
<td>2 K</td>
</tr>
<tr>
<td>IPv4 QoS classification</td>
<td>4 K</td>
<td>4 K</td>
</tr>
</tbody>
</table>

Table 8-3 shows the approximate number of each resource supported in each of the templates for a switch running the Scaled metro aggregation services image.

Table 8-3  
**Approximate Number of Feature Resources Allowed by Each Template**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default</th>
<th>VPNv4 Only SDM Template</th>
<th>VPNv4-v6 SDM Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC table</td>
<td>256K</td>
<td>256K</td>
<td>256K</td>
</tr>
<tr>
<td>IPv4 routes</td>
<td>32 K</td>
<td>80 K</td>
<td>80 K</td>
</tr>
<tr>
<td>IPv6 routes</td>
<td>16 K</td>
<td>8 K</td>
<td>40 K</td>
</tr>
<tr>
<td>IPv4 Routing Groups</td>
<td>4 K</td>
<td>8 K</td>
<td>2 K</td>
</tr>
<tr>
<td>Multicast Groups</td>
<td>4 K</td>
<td>4 K</td>
<td>2 K</td>
</tr>
<tr>
<td>Bridge Domains</td>
<td>8 K</td>
<td>4 K</td>
<td>8 K</td>
</tr>
<tr>
<td>Ethernet Flow Point (EFP)</td>
<td>16 K</td>
<td>4 K</td>
<td>4 K</td>
</tr>
<tr>
<td>ACL entries</td>
<td>16 K</td>
<td>4 K</td>
<td>4 K</td>
</tr>
<tr>
<td>IPv4 QoS classification</td>
<td>24 K</td>
<td>12 K</td>
<td>12 K</td>
</tr>
</tbody>
</table>
Configuring the Switch SDM Template

- SDM Template Configuration Guidelines, page 8-3
- Setting the SDM Template, page 8-3

SDM Template Configuration Guidelines

Follow these guidelines when selecting and configuring SDM templates:

- You must reload the switch for the configuration to take effect.

Setting the SDM Template

In the privileged EXEC mode, perform these steps to use the SDM templates to select a template on the switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enter the privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 2 sdm prefer {default</td>
<td>vpnv4-only vpv4-v6}</td>
</tr>
<tr>
<td></td>
<td>The keywords have these meanings:</td>
</tr>
<tr>
<td></td>
<td>- default—Balance all functions.</td>
</tr>
<tr>
<td></td>
<td>- Vpnv4-only—VPNv4 template.</td>
</tr>
<tr>
<td></td>
<td>- Vpnv4-v6—VPNv4-v6 template.</td>
</tr>
<tr>
<td>Step 3 sdm prefer {default</td>
<td>ip}</td>
</tr>
<tr>
<td></td>
<td>- default—Balance all functions.</td>
</tr>
<tr>
<td></td>
<td>- ip—Increased ipv4</td>
</tr>
<tr>
<td>Step 4 sdm prefer {default</td>
<td>ip}</td>
</tr>
<tr>
<td></td>
<td>- default—Balance all functions.</td>
</tr>
<tr>
<td></td>
<td>- ip—Increased ipv4</td>
</tr>
<tr>
<td>Step 5 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6 reload</td>
<td>Reload the operating system.</td>
</tr>
</tbody>
</table>

After the system reboots, you can use the show sdm prefer current command in the privileged EXEC mode to verify the new template configuration. If you enter the show sdm prefer current command before you enter the reload privileged EXEC command, the show sdm prefer current command shows the template currently in use and the template that will become active after a reload.

This example shows how to configure a switch with the vpnv4-only template.

Switch# sdm prefer vpnv4-only
Switch# end
Switch# reload
Proceed with reload? [confirm]

This is an example of an output display for the SCALED METRO AGG Services licence:

Switch# show sdm prefer current
The current License is ScaledMetroAggrServices
The current template is "default" template.

Template values:
number of mac table entries = 256000
number of ipv4 routes = 32000
number of ipv6 routes = 16000
number of routing groups = 4000
number of multicast groups = 4000
number of bridge domains = 8192
number of acl entries = 16000
On next reload, template will be "VPNv4-only" template.

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

Displaying the SDM Templates

Use the show sdm prefer current privileged EXEC command to display the active template. Use the show sdm prefer \{default\ | vpnv4-v6 | vpnv4-only\} 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, where the SCALED METRO AGGREGATION SERVICES license is being used:

Switch# show sdm prefer?
current show current template configuration
default show default template configuration
Vpnv4-v6 show VPNv4-v6 template configuration
Vpnv4-only show VPNv4 template configuration

Switch#show sdm prefer default
The current License is ScaledMetroAggrServices
default template:

Template values:
number of mac table entries = 256000
number of ipv4 routes = 32000
number of ipv6 routes = 16000
number of routing groups = 4000
number of multicast groups = 4000
number of bridge domains = 8192
number of acl entries = 16000

Switch# show sdm prefer current
The current License is ScaledMetroAGGrServices.
The current template is "default" template.
Template values:
number of mac table entries = 256000
number of ipv4 routes = 32000
number of ipv6 routes = 16000
number of routing groups = 4000
number of multicast groups = 4000
number of bridge domains = 8192
number of acl entries = 16000

Switch# show sdm prefer vpnv4-only
The current License is ScaledMetroAggrServices Vpnv4-only template:
Template values:
number of mac table entries = 256000
number of ipv4 routes = 80000
number of ipv6 routes = 8000
number of routing groups = 8000
number of multicast groups = 4000
number of bridge domains = 8192
number of acl entries = 4000

Switch# show sdm prefer vpnv4-v6
The current License is ScaledMetroAggrServices Vpnv4-v6 template:
Template values:
number of mac table entries = 256000
number of ipv4 routes = 80000
number of ipv6 routes = 4000
number of routing groups = 2000
number of multicast groups = 2000
number of bridge domains = 8192
number of acl entries = 4000
Displaying the SDM Templates
This chapter describes how to configure switch-based authentication on the Cisco ME 3800X and ME 3600X switch.

- Preventing Unauthorized Access to Your Switch, page 9-1
- Protecting Access to Privileged EXEC Commands, page 9-2
- Controlling Switch Access with TACACS+, page 9-10
- Controlling Switch Access with RADIUS, page 9-17
- Controlling Switch Access with Kerberos, page 9-31
- Configuring the Switch for Local Authentication and Authorization, page 9-35
- Configuring the Switch for Secure Shell, page 9-36
- Configuring the Switch for Secure Copy Protocol, page 9-39

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 9-2.

- 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 9-6.
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.

For complete syntax and usage information for the commands used in this section, see the Cisco IOS Security Command Reference, Release 12.4.

- Default Password and Privilege Level Configuration, page 9-2
- Setting or Changing a Static Enable Password, page 9-3
- Protecting Enable and Enable Secret Passwords with Encryption, page 9-3
- Disabling Password Recovery, page 9-5
- Setting a Telnet Password for a Terminal Line, page 9-6
- Configuring Username and Password Pairs, page 9-6
- Configuring Multiple Privilege Levels, page 9-7

Default Password and Privilege Level Configuration

Table 9-1 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). 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). 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>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 enable password</td>
<td>Define a new password or change an existing password for access to privileged EXEC mode. By default, no password is defined. For password, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. It can contain the question mark (?) character if you precede the question mark with the key combination Ctrl-v when you create the password; for example, to create the password abc?123, do this: Enter abc. Enter Ctrl-v. Enter ?123. When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-v; you can simply enter abc?123 at the password prompt.</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</td>
<td>(Optional) Save your entries in the configuration file. 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 Trivial File Transfer Protocol (TFTP) server, you can use either the enable password or enable secret global configuration commands. Both commands accomplish the same thing; that is, you can establish an encrypted password that users must enter to access privileged EXEC mode (the default) or any privilege level you specify.

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

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

<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>enable password [level level] {password</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>service password-encryption</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>copy running-config startup-config</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 9-7.

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$Xyti5Rklz3Loysz8 for privilege level 2:

```
Switch(config)# enable secret level 2 5 $1$FaD0$Xyti5Rklz3Loysz8
```

## 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. 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 37-2.

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

<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 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>3</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>4</td>
<td>show version</td>
<td>Verify the configuration by checking the last few lines of the command output.</td>
</tr>
</tbody>
</table>

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

**Note**

Disabling password recovery will 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.
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>
<tbody>
<tr>
<td>Step 1</td>
<td>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.</td>
</tr>
<tr>
<td>Step 2</td>
<td>enter privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>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.</td>
</tr>
<tr>
<td>Step 5</td>
<td>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.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Verify your entries. The password is listed under the command line vty 0 15.</td>
</tr>
<tr>
<td>Step 8</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

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 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 2</td>
<td>username name [privilege level]</td>
<td>Enter the username, privilege level, and password for each user.</td>
</tr>
<tr>
<td></td>
<td>{password encryption-type password}</td>
<td></td>
</tr>
<tr>
<td></td>
<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></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 1 gives user EXEC mode access.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For encryption-type, enter 0 to specify that an unencrypted password will follow. Enter 7 to specify that a hidden password will follow.</td>
</tr>
<tr>
<td></td>
<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>Step 3</td>
<td>line console 0</td>
<td>Enter line configuration mode, and configure the console port (line 0) or the VTY lines (line 0 to 15).</td>
</tr>
<tr>
<td></td>
<td>or line vty 0 15</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>login local</td>
<td>Enable local password checking at login time. Authentication is based on the username specified in Step 2.</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 running-config</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 disable username authentication for a specific user, use the no username name global configuration command. To disable password checking and allow connections without a password, use the no login line configuration command.

### Configuring Multiple Privilege Levels

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

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

These sections contain this configuration information:

- Setting the Privilege Level for a Command, page 9-8
- Changing the Default Privilege Level for Lines, page 9-9
- Logging into and Exiting a Privilege Level, page 9-9
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 configuration mode, exec for EXEC mode, interface for interface configuration mode, or line for line configuration mode.</td>
</tr>
<tr>
<td></td>
<td>• For level, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. Level 15 is the level of access permitted by the enable password.</td>
</tr>
<tr>
<td></td>
<td>• For command, specify the command to which you want to restrict access.</td>
</tr>
<tr>
<td>Step 3  enable password level level password</td>
<td>Specify the enable password for the privilege level.</td>
</tr>
<tr>
<td></td>
<td>• For level, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges.</td>
</tr>
<tr>
<td></td>
<td>• 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.</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></td>
<td>The first command shows the password and access level configuration.</td>
</tr>
<tr>
<td></td>
<td>The second command shows the privilege level 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>

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 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>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 line vty line</td>
<td>Select the virtual terminal line on which to restrict access.</td>
</tr>
<tr>
<td>Step 3 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>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 show privilege</td>
<td>The first command shows the password and access level 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>

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>Step 1 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>Step 2 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 Terminal Access Controller Access Control System Plus (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.

- Understanding TACACS+, page 9-10
- TACACS+ Operation, page 9-12
- Configuring TACACS+, page 9-12
- Displaying the TACACS+ Configuration, page 9-17

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—individually. 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 9-1.
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 to show 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 dialog 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.

The `aaa authorization console` global configuration command that allows you to enable AAA and TACACS+ to work on the console port.

These sections contain this configuration information:
- Default TACACS+ Configuration, page 9-13
- Identifying the TACACS+ Server Host and Setting the Authentication Key, page 9-13
- Configuring TACACS+ Login Authentication, page 9-14
- Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services, page 9-16
- Starting TACACS+ Accounting, page 9-16

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:

<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>tacacs-server host hostname [port integer] [timeout integer] [key string]</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></td>
<td></td>
<td>• For hostname, specify the name or IP address of the host.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For port integer, specify a server port number. The default is port 49. The range is 1 to 65535.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For timeout integer, 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>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For key string, 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>
</tr>
</tbody>
</table>

<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>
Chapter 9  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 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>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>aaa new-model</td>
<td>Enable AAA.</td>
</tr>
</tbody>
</table>

### Command Purpose

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>aaa group server tacacs+ group-name</td>
<td>(Optional) Define the AAA server-group with a group name. This command puts the switch in a server group subconfiguration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>server ip-address</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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</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>Step 7</td>
<td>show tacacs</td>
<td>Verify your entries.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 8</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
## 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.

### Step 3

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.

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 tacacs+**—Uses TACACS+ authentication. Before you can use this authentication method, you must configure the TACACS+ server. For more information, see the “Identifying the TACACS+ Server Host and Setting the Authentication Key” section on page 9-13.
- **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 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

Enter line configuration mode, and configure the lines to which you want to apply the authentication list.

### Step 5

Apply the authentication list to a line or set of lines.
- If you specify `default`, use the default list created with the `aaa authentication login` command.
- For `list-name`, specify the list created with the `aaa authentication login` command.

### Step 6

Return to privileged EXEC mode.

### Step 7

Verify your entries.

### Step 8

(Optional) Save your entries in the configuration file.

---

### Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>`aaa authentication login {default</td>
</tr>
<tr>
<td></td>
<td>- To create a default list that is used when a named list is not 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>
<tr>
<td></td>
<td>Select one of these methods:</td>
</tr>
<tr>
<td></td>
<td>- <strong>enable</strong>—Use the enable password for authentication. Before you can use this authentication method, you must define an enable password by using the <code>enable password</code> global configuration command.</td>
</tr>
<tr>
<td></td>
<td>- <strong>group tacacs+</strong>—Uses TACACS+ authentication. Before you can use this authentication method, you must configure the TACACS+ server. For more information, see the “Identifying the TACACS+ Server Host and Setting the Authentication Key” section on page 9-13.</td>
</tr>
<tr>
<td></td>
<td>- <strong>line</strong>—Use the line password for authentication. Before you can use this authentication method, you must define a line password. Use the <code>password password</code> line configuration command.</td>
</tr>
<tr>
<td></td>
<td>- <strong>local</strong>—Use the local username database for authentication. You must enter username information in the database. Use the <code>username password</code> global configuration command.</td>
</tr>
<tr>
<td></td>
<td>- <strong>local-case</strong>—Use a case-sensitive local username database for authentication. You must enter username information in the database by using the <code>username name password</code> global configuration command.</td>
</tr>
<tr>
<td></td>
<td>- <strong>none</strong>—Do not use any authentication for login.</td>
</tr>
<tr>
<td></td>
<td>Step 4</td>
</tr>
<tr>
<td></td>
<td>Step 5</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Step 6</td>
</tr>
<tr>
<td></td>
<td>Step 7</td>
</tr>
<tr>
<td></td>
<td>Step 8</td>
</tr>
</tbody>
</table>
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><code>aaa authorization network tacacs+</code></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>aaa authorization exec tacacs+</code></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>end</code></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>show running-config</code></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>copy running-config startup-config</code></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>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 network start-stop tacacs+</td>
<td>Enable TACACS+ accounting for all network-related service requests.</td>
</tr>
<tr>
<td>Step 3 aaa accounting exec start-stop tacacs+</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>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 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.

**Note**

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

These sections contain this configuration information:

- Understanding RADIUS, page 9-17
- RADIUS Operation, page 9-19
- Configuring RADIUS, page 9-19
- Displaying the RADIUS Configuration, page 9-30

**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 9-2 on page 9-18.
- 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.
- 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.

**Figure 9-2 Transitioning from RADIUS to TACACS+ Services**

![Figure 9-2 Transitioning from RADIUS to TACACS+ Services](image)
**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.

These sections contain this configuration information:

- Default RADIUS Configuration, page 9-20
- Identifying the RADIUS Server Host, page 9-20 (required)
- Configuring RADIUS Login Authentication, page 9-22 (required)
- Defining AAA Server Groups, page 9-24 (optional)
- Configuring RADIUS Authorization for User Privileged Access and Network Services, page 9-26 (optional)
- Starting RADIUS Accounting, page 9-27 (optional)
- Configuring Settings for All RADIUS Servers, page 9-28 (optional)
- Configuring the Switch to Use Vendor-Specific RADIUS Attributes, page 9-28 (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.

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 9-24.
Beginning in privileged EXEC mode, follow these steps to configure per-server RADIUS server communication. 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 authentication.</td>
</tr>
<tr>
<td>Step 3</td>
<td></td>
</tr>
<tr>
<td>radius-server host [hostname</td>
<td>Specify the IP address or hostname of the remote RADIUS server host.</td>
</tr>
<tr>
<td>ip-address] [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]</td>
<td>(Optional) For auth-port port-number, specify the UDP destination port for authentication requests.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Optional) For acct-port port-number, specify the UDP destination port for accounting requests.</td>
</tr>
<tr>
<td></td>
<td>(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.</td>
</tr>
<tr>
<td></td>
<td>(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.</td>
</tr>
<tr>
<td></td>
<td>(Optional) For key string, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td>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.</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 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:

```bash
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:

```bash
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><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td><code>aaa new-model</code></td>
<td>Enable AAA.</td>
</tr>
</tbody>
</table>
### Step 3

**Command**

```text
aaa authentication login {default | list-name} method1 [method2...]
```

**Purpose**

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.

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 9-20.

- **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 password` global configuration command.

- **none**—Do not use any authentication for login.

### Step 4

**Command**

```text
line [console | tty | vty] line-number
[ending-line-number]
```

**Purpose**

Enter line configuration mode, and configure the lines to which you want to apply the authentication list.
Controlling Switch Access with RADIUS

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>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>radius-server host {hostname</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>aaa new-model</td>
</tr>
<tr>
<td>Step 4</td>
<td>aaa group server radius group-name</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>server ip-address</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
</tr>
<tr>
<td>Step 7</td>
<td>show running-config</td>
</tr>
</tbody>
</table>
Controlling Switch Access with RADIUS

Chapter 9      Configuring Switch-Based Authentication

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
Enter global configuration mode.

Step 2
aaa authorization network radius
Configure the switch for user RADIUS authorization for all network-related service requests.
```

<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>
<tr>
<td><code>enable radius login authentication</code></td>
<td>Enable RADIUS login authentication. See the “Configuring RADIUS Login Authentication” section on page 9-22.</td>
</tr>
</tbody>
</table>
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>Step 1</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>aaa accounting network start-stop radius</code></td>
<td>Enable RADIUS accounting for all network-related service requests.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>aaa accounting exec start-stop radius</code></td>
<td>Enable RADIUS 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>Step 4</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>show running-config</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 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>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>radius-server key <code>string</code></td>
<td>Specify the shared secret text string used between the switch and all RADIUS servers.</td>
</tr>
<tr>
<td></td>
<td>Note The key is a text string that must match the encryption key used on the RADIUS server. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.</td>
</tr>
<tr>
<td>radius-server retransmit <code>retries</code></td>
<td>Specify the number of times the switch sends each RADIUS request to the server before giving up. The default is 3; the range 1 to 1000.</td>
</tr>
<tr>
<td>radius-server timeout <code>seconds</code></td>
<td>Specify the number of seconds a switch waits for a reply to a RADIUS request before resending the request. The default is 5 seconds; the range is 1 to 1000.</td>
</tr>
<tr>
<td>radius-server deadtime <code>minutes</code></td>
<td>Specify the number of minutes a RADIUS server, which is not responding to authentication requests, to be skipped, thus avoiding the wait for the request to timeout before trying the next configured server. The default is 0; the range is 1 to 1440 minutes.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Verify your settings.</td>
</tr>
<tr>
<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 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"
```
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 an interface 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 an interface 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>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| radius-server vsa send [accounting | Enable the switch to recognize and use VSAs as defined by RADIUS IETF authentication] attribute 26.  
  | authentication]         |   • (Optional) Use the accounting keyword to limit the set of recognized vendor-specific attributes to only accounting attributes.  
   |                          |   • (Optional) Use the authentication keyword to limit the set of recognized vendor-specific attributes to only authentication attributes.  
   |                          | If you enter this command without keywords, both accounting and authentication vendor-specific attributes are used. |
| end                      | Return to privileged EXEC mode.                                         |
| show running-config      | Verify your settings.                                                   |
| copy running-config startup-config | (Optional) Save your entries in the configuration file.                |

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>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>radius-server host {hostname</td>
<td>ip-address} non-standard</td>
</tr>
<tr>
<td>radius-server key string</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. <strong>Note</strong> The key is a text string that must match the encryption key used on the RADIUS server. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Verify your settings.</td>
</tr>
<tr>
<td>copy running-config startup-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 \{hostname | ip-address\} non-standard` global configuration command. To disable the key, use the `no radius-server key` global configuration command.

This example shows how to specify a vendor-proprietary RADIUS host and to use a secret key of `rad124` between the 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.

These sections contain this information:

- Understanding Kerberos, page 9-31
- Kerberos Operation, page 9-33
- Configuring Kerberos, page 9-34

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 Cisco IOS Security Command Reference, Release 12.4, 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 Cisco ME 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 Cisco ME 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.

The switch 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).
Kerberos supports these network services:

- Telnet
- rlogin
- rsh (Remote Shell Protocol)

Table 9-2 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 TGTs(^1) 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 eight 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. Note The Kerberos principal and instance names must be in all lowercase characters. Note The Kerberos realm name must be in all uppercase characters.</td>
</tr>
<tr>
<td>KDC(^2)</td>
<td>Key distribution center 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. Note 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>
</tbody>
</table>

Note The Kerberos realm name must be in all uppercase characters.
Controlling Switch Access with Kerberos

Kerberos Operation

A Kerberos server can be a Cisco ME 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 Cisco ME switch as a Kerberos server, remote users must follow these steps:

1. **Authenticating to a Boundary Switch, page 9-33**
2. **Obtaining a TGT from a KDC, page 9-34**
3. **Authenticating to Network Services, page 9-34**

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.

### Table 9-2 Kerberos Terms (continued)

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEYTAB³</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 KEYTAB to decrypt it. In Kerberos versions earlier than Kerberos 5, KEYTAB is referred to as SRVTAB⁴.</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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The Kerberos principal name must be in all lowercase characters.</td>
</tr>
<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>

---

³ KEYTAB

⁴ SRVTAB
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.

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 “Security Server Protocols” chapter 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 “Security Server Protocols” chapter 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.

A Kerberos server can be a Cisco ME 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 “Security Server Protocols” chapter 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></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>aaa new-model</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>aaa authentication login default local</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>aaa authorization exec local</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>aaa authorization network local</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>username <em>name</em> [privilege <em>level</em>] {password <em>encryption-type</em> <em>password</em>}</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>end</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>copy running-config startup-config</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} method1** global configuration command.
Configuring the Switch for Secure Shell

This section describes how to configure the Secure Shell (SSH) feature. To use this feature, you must install the cryptographic (encrypted) software image 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.

These sections contain this information:

- Understanding SSH, page 9-36
- Configuring SSH, page 9-37
- Displaying the SSH Configuration and Status, page 9-39

For SSH configuration examples, see the “SSH Configuration Examples” section in the “Configuring Secure Shell” chapter 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 Cisco IOS Security Command Reference 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 9-36
- Limitations, page 9-37

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 9-10)
- RADIUS (for more information, see the “Controlling Switch Access with RADIUS” section on page 9-17)
Local authentication and authorization (for more information, see the “Configuring the Switch for Local Authentication and Authorization” section on page 9-35)

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 does not support the Advanced Encryption Standard (AES) symmetric encryption algorithm.

Configuring SSH
This section has this configuration information:

- Configuration Guidelines, page 9-37
- Setting Up the Switch to Run SSH, page 9-37 (required)
- Configuring the SSH Server, page 9-38 (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 9-37.
- 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 9-35.

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>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>hostname hostname</td>
<td>Configure a hostname for your switch.</td>
</tr>
<tr>
<td>Step 3</td>
<td></td>
</tr>
<tr>
<td>ip domain-name domain_name</td>
<td>Configure a host domain for your switch.</td>
</tr>
<tr>
<td>Step 4</td>
<td></td>
</tr>
<tr>
<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. We recommend that a minimum modulus size of 1024 bits. 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>Step 5</td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td></td>
</tr>
<tr>
<td>show ip ssh</td>
<td>Show the version and configuration information for your SSH server.</td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>show ssh</td>
<td>Show the status of the SSH server on the switch.</td>
</tr>
<tr>
<td>Step 7</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 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>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>ip ssh version [1</td>
<td>2]</td>
</tr>
<tr>
<td></td>
<td>• 1—Configure the switch to run SSH Version 1.</td>
</tr>
<tr>
<td></td>
<td>• 2—Configure the switch to run SSH Version 2.</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>
</tbody>
</table>
To return to the default SSH control parameters, use the `no ip ssh` 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 9-3:

<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>or <code>show ssh</code></td>
<td>Shows the status of the SSH server connections on the switch.</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>

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 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" section in the Cisco IOS Security Configuration Guide: Securing User Services, Release 12.4.

Configuring Interfaces

This chapter defines the types of interfaces on the Cisco ME 3800X and ME 3600X switches and describes how to configure them.

- Understanding Interface Types, page 10-1
- Using Interface Configuration Mode, page 10-6
- Using the Ethernet Management Port, page 10-10
- Configuring Ethernet Interfaces, page 10-13
- Configuring Layer 3 Interfaces, page 10-19
- Configuring the Interface MTU, page 10-20
- Monitoring and Maintaining the Interfaces, page 10-21

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.

- NNI Port Type, page 10-2
- Port-Based VLANs, page 10-2
- Switch Ports, page 10-2
- Routed Ports, page 10-3
- Ethernet Management Port, page 10-4
- Switch Virtual Interfaces, page 10-4
- EtherChannel Port Groups, page 10-4
- Connecting Interfaces, page 10-5
### NNI Port Type

All Cisco ME 3800X and 3600X ports are network node interfaces (NNIs), which are typically connected to a router or to another switch. The default status for an NNI is administratively up to allow a service provider remote access to the switch during initial configuration.

### 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 associated with the VLAN ID or when a user creates the VLAN ID.

To configure VLANs, use the `vlan vlan-id` global configuration command to enter VLAN configuration mode. The VLAN configurations for VLAN IDs 1 to 1005 are saved in the VLAN database. Extended-range VLANs (VLAN IDs 1006 to 4094) are not added to the VLAN database. 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.

To isolate VLANs of different customers in a service-provider network, Cisco ME switches use UNI VLANs. Local switching does not occur among user network interfaces (UNIs) and enhanced network interfaces (ENIs) on the switch that belong to the same UNI isolated VLAN. Local switching is allowed among ports that belong to a UNI community VLAN. Because all ports on the ME 3800X and 3600X switches are NNIs, UNI VLAN configuration has no effect. Local switching is allowed between NNIs.

### Switch Ports

Switch ports are Layer 2 only interfaces associated with a physical port. Switch ports belong to one or more VLANs. You can configure a port as an access port or 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. Use the `switchport` command with no keywords to put an interface that is in Layer 3 mode into Layer 2 mode.

---

**Note**

When you put an interface that is in Layer 3 mode into Layer 2 mode, the previous configuration information related to the affected interface might be lost, and the interface is returned to its default configuration.

For detailed information about configuring access port and trunk port characteristics, see Chapter 11, “Configuring VLANs.”
Access Ports

An access port belongs to and carries the traffic of only one VLAN. 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 an IEEE 802.1Q tagged packet, the packet is dropped, and the source address is not learned. IEEE 802.1x can also be used for VLAN assignment.

You manually assign static access ports to a VLAN.

Trunk Ports

An IEEE 802.1Q trunk port carries the traffic of multiple VLANs and by default is a member of all VLANs in the VLAN database. A trunk port supports simultaneous tagged and untagged traffic. An IEEE 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 multiple VLANs, 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 become a member of a VLAN only if the VLAN is in the enabled state.

For more information about trunk ports, see Chapter 11, “Configuring VLANs.”

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 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.

Note

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. When you put an interface that is in Layer 2 mode into Layer 3 mode, the previous configuration information related to the affected interface might be lost.

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 10-19 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 29, “Configuring IP Unicast Routing” and Chapter 35, “Configuring IP Multicast Routing.”
Understanding Interface Types

Ethernet Management Port

The Ethernet management port, also referred to as the Gi0 or gigabitethernet0 port, is a Layer 3 host port to which you can connect a PC. You can use the Ethernet management port instead of the switch console port for network management.

See the “Using the Ethernet Management Port” section on page 10-10 for more information.

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 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.

Note

You cannot delete interface VLAN 1.

SVIs provide IP host connectivity only to the system; in Layer 3 mode, you can configure routing across SVIs.

Although the switch supports a total of 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 10-19 for information about what happens when hardware resource limitations are reached.

SVIs are created the first time that you enter the vlan interface configuration command for a VLAN interface. The VLAN corresponds to the VLAN tag associated with data frames on an IEEE 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 3-15.

Note

When you create an SVI, it does not become active until it is associated with a physical port.

SVIs support routing protocols. For more information about configuring IP routing, see Chapter 29, “Configuring IP Unicast Routing,” and Chapter 35, “Configuring IP Multicast Routing.”

EtherChannel Port Groups

EtherChannel port groups 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, 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 Cisco Discovery Protocol (CDP), Link Aggregation Control Protocol (LACP), and the Port Aggregation Protocol (PAgP), which operate only on physical NNI or ENI 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 **interface port-channel** global configuration command. Then you manually assign an interface to the EtherChannel by using the **channel-group** interface configuration command. For Layer 2 interfaces, use the **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 28, “Configuring EtherChannels.”

**Ethernet Flow Points**

An Ethernet Flow Point (EFP) is a logical interface that connects an Ethernet Virtual Connection (EVC) bridge domain to a physical port in a switch. Configuring a service instance on an interface creates a pseudoport or EFP on which you configure EVC features.

You can configure EFP service instances only on Layer 2 ports. You can configure an EtherChannel with a service instance, but you cannot add an interface to a channel group if it has a service instance configured on it. EFPs do not support routing. EFPs do not support **switchport** commands.

Switch interfaces configured with service instances support a different range of features than interfaces that do not have service instances. For more information on EVCs, see Chapter 12, “Configuring Ethernet Virtual Connections (EVCs).”

**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. By using the switch with routing enabled, when you configure both VLAN 20 and VLAN 30 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 10-1).

![Figure 10-1 Connecting VLANs with the Switch](image-url)

You can enable routing on all SVIs and routed ports on the switch. 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. 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 29, “Configuring IP Unicast Routing” and Chapter 35, “Configuring IP Multicast Routing.”

## Using Interface Configuration Mode

The switch supports these interface types:

- Physical ports—switch ports, routed ports
- SVIs—switch virtual interfaces
- Port-channels—EtherChannel interfaces

**Note**

The switch also supports EFP service instances configured on physical interfaces. You configure EFPs in service-instance configuration mode. See Chapter 12, “Configuring Ethernet Virtual Connections (EVCs).”

You can also configure a range of interfaces (see the “Configuring a Range of Interfaces” section on page 10-7).

To configure a physical interface (port), specify the interface type, the module number, and the switch port number, and enter interface configuration mode.

- **Type**—Gigabit Ethernet (gigabitethernet or gi) for 10/100/1000 Mb/s Ethernet ports, or small form-factor pluggable (SFP) module Gigabit Ethernet interfaces.
- **Module number**—The module or slot number on the switch (always 0 on the Cisco ME switch).
- **Port number**—The interface number on the switch. The port numbers always begin at 1, starting with the leftmost port when facing the front of the switch, for example, gigabitethernet 0/1. If there is more than one interface type (for example, 10/100/1000 ports and SFP module ports), the port numbers restart with the second interface type: gigabitethernet 0/1.

You can identify physical interfaces by physically checking the interface location on the switch. You can also use the `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 the number of the connector. In this example, Fast Ethernet port 1 is selected:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)#
```
You do not need to add a space between the interface type and interface number. For example, in the preceding line, you can specify either `gigabitethernet 0/1`, `gigabitethernet0/1`, `gi 0/1`, or `gi0/1`.

**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 10-21.

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> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> interface range <code>{port-range}</code></td>
<td>Specify the range of interfaces (VLANs or physical ports) to be configured, and enter interface range configuration mode.</td>
</tr>
<tr>
<td></td>
<td>• You can use the <code>interface range</code> command to configure up to five port ranges or a previously defined macro.</td>
</tr>
<tr>
<td></td>
<td>• In a comma-separated <code>port-range</code>, you must enter the interface type for each entry and enter spaces before and after the comma.</td>
</tr>
<tr>
<td></td>
<td>• In a hyphen-separated <code>port-range</code>, you do not need to re-enter the interface type, but you must enter a space before the hyphen.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>You can now use the normal configuration commands to apply the configuration parameters to all interfaces in the range.</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 interfaces <code>[interface-id]</code></td>
<td>Verify the configuration of the interfaces in the range.</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>

When using the `interface range` global configuration command, note these guidelines:

- Valid entries for `port-range`:
Using Interface Configuration Mode

Chapter 10  Configuring Interfaces

Using Interface Configuration Mode

- `vlan vlan-ID - vlan-ID`, where the VLAN ID is 1 to 4094
- `gigabitethernet module/{first port} - {last port}`, where the module is always 0
- `tengigabitethernet module/{first port} - {last port}`, where the module is always 0
- `port-channel port-channel-number - port-channel-number`, where the `port-channel-number` is 1 to 26

Note When you use the `interface range` command with port channels, the first and last port channel number must be active port channels.

- 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 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 ports 1 and 2 to 100 Mb/s:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 - 2
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 1 to 3 and Gigabit Ethernet ports 1 and 2 to receive IEEE 802.3x flow control pause frames:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 - 3, gigabitethernet0/5 - 6
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:
Using Interface Configuration Mode

Use the **no define interface-range macro_name** global configuration command to delete a macro.

When using the **define interface-range macro_name** global configuration command, note these guidelines:

- **Valid entries for interface-range:**
  - `vlan vlan-ID - vlan-ID`, where the VLAN ID is 1 to 4094
  - `gigabitethernet module/{first port} - {last port}`, where the module is always 0
  - `tengigabitethernet module/{first port} - {last port}`, where the module is always 0
  - `port-channel port-channel-number - port-channel-number`, where the port-channel-number is 1 to 26.

**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, `gigabitethernet0/1 - 2` is a valid range; `gigabitethernet0/1-2` 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 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 named `enet_list` to include ports 1 and 2 and to verify the macro configuration:

```
Switch# configure terminal
Switch(config)# define interface-range enet_list gigabitethernet0/1 - 2
Switch(config)# end
Switch# show running-config | include define
define interface-range enet_list GigabitEthernet0/1 - 2
```
This example shows how to create a multiple-interface macro named macro1 and assign all of the interfaces in the range to a VLAN:

Switch# configure terminal
Switch(config)# define interface-range macro1 gigabitethernet0/1 - 2, gigabitethernet0/5 - 6
Switch(config)# interface range macro macro1
Switch(config-if-range)# switchport access vlan 20
Switch(config-if-range)# 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#

Using the Ethernet Management Port

- Understanding the Ethernet Management Port, page 10-10
- Supported Features on the Ethernet Management Port, page 10-12
- Configuring the Ethernet Management Port, page 10-12
- TFTP and the Ethernet Management Port, page 10-12

Understanding the Ethernet Management Port

The Ethernet management port is port Gi0 or gigabitethernet0, a Layer 3 host port to which you can connect a PC. You can use the Ethernet management port instead of the switch console port for network management.

Note

You cannot configure an EFP service instance on the Ethernet management port.

When connecting a PC to the Ethernet management port, you must assign an IP address. Connect the Ethernet management port to the PC as shown in Figure 10-2.
By default, the Ethernet management port is enabled. The switch cannot route packets from the Ethernet management port to a network port or receive routed packets from a network port.

Even though the Ethernet management port does not support routing, you might need to enable routing protocols on the port. For example, in Figure 10-3, you must enable routing protocols on the Ethernet management port when the PC is two or more hops away from the switch and the packets must pass through two or more Layer 3 devices to reach the PC.

In Figure 10-3, if the Ethernet management port and the network ports are associated with the same routing process, the routes are propagated in this manner:

- The routes from the Ethernet management port are propagated through the network ports to the network.
- The routes from the network ports are propagated through the Ethernet management port to the network.

Because routing is not supported between the Ethernet management port and the network ports, traffic cannot be sent or received between these ports. If traffic is sent or received, data packet loops occur between the ports, which disrupts the switch and network operation. Configure route filters to avoid routes between the Ethernet management port and the network ports and to prevent the loops.
Supported Features on the Ethernet Management Port

The Ethernet management port supports these features:

- Telnet with passwords
- TFTP
- Secure Shell (SSH)
- DHCP-based autoconfiguration
- SMNP (only the ENTITY-MIB and the IF-MIB)
- IP ping
- Interface features
- Speed—1000 Mb/s, and autonegotiation
- Duplex mode—Full, half, and autonegotiation
- Loopback detection
- Cisco Discovery Protocol (CDP)
- DHCP relay agent
- IPv4 access control lists (ACLs)
- Routing protocols

Caution
Before enabling a feature on the Ethernet management port, make sure that the feature is supported. If you try to configure an unsupported feature on the Ethernet Management port, the feature might not work properly, and the switch might fail.

Configuring the Ethernet Management Port

To specify the Ethernet management port in the CLI, enter `gigabitethernet0`.

To disable the port, use the `shutdown` interface configuration command. To enable the port, use the `no shutdown` interface configuration command.

You can monitor the Ethernet management port LED to determine the link status to the PC. The LED is green (on) when the link is active, and the LED is off when the link is down. The LED is amber when there is a POST failure.

To display the link status, use the `show interfaces gigabitethernet 0` privileged EXEC command.

TFTP and the Ethernet Management Port

Use the commands in Table 1 when using TFTP to download or upload a configuration file to the boot loader.
### Default Ethernet Interface Configuration

Table 10-2 shows the Ethernet interface default configuration. 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 20, “Configuring Traffic Control.”

#### 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. When you put an interface that is in Layer 3 mode into Layer 2 mode, the previous configuration information related to the affected interface might be lost, and the interface is returned to its default configuration.

### Configuring Ethernet Interfaces

- Default Ethernet Interface Configuration, page 10-13
- Configuring Interface Speed and Duplex Mode, page 10-14
- Configuring IEEE 802.3x Flow Control, page 10-16
- Configuring Auto-MDIX on an Interface, page 10-17
- Adding a Description for an Interface, page 10-18

#### Table 1 Boot Loader Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>arp [ip_address]</code></td>
<td>Displays the currently cached ARP(^1) table when this command is entered without the <code>ip_address</code> parameter. Enables ARP to associate a MAC address with the specified IP address when this command is entered with the <code>ip_address</code> parameter.</td>
</tr>
<tr>
<td><code>mgmt_clr</code></td>
<td>Clears the statistics for the Ethernet management port.</td>
</tr>
<tr>
<td><code>mgmt_init</code></td>
<td>Starts the Ethernet management port.</td>
</tr>
<tr>
<td><code>mgmt_show</code></td>
<td>Displays the statistics for the Ethernet management port.</td>
</tr>
<tr>
<td><code>ping host_ip_address</code></td>
<td>Sends ICMP ECHO_REQUEST packets to the specified network host.</td>
</tr>
<tr>
<td><code>boot tftp:/file-url ...</code></td>
<td>Loads and boots an executable image from the TFTP server and enters the command-line interface. For more details, see the command reference for this release.</td>
</tr>
<tr>
<td><code>copy tftp:source-file-url filesystem:/destination-file-url</code></td>
<td>Copies a Cisco IOS image from the TFTP server to the specified location. For more details, see the command reference for this release.</td>
</tr>
</tbody>
</table>

1. ARP = Address Resolution Protocol.
Configuring Ethernet Interfaces

Table 10-2  Default Ethernet 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 IEEE 802.1Q trunks)</td>
<td>VLAN 1 (Layer 2 interfaces only).</td>
</tr>
<tr>
<td>VLAN trunking</td>
<td>Switchport mode access (Layer 2 interfaces only).</td>
</tr>
<tr>
<td>Port enable state</td>
<td>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>IEEE 802.3x flow control</td>
<td>Flow control is set to receive: off. It is always off for sent packets.</td>
</tr>
<tr>
<td>EtherChannel</td>
<td>Disabled on all Ethernet ports. See Chapter 28, “Configuring EtherChannels.”</td>
</tr>
<tr>
<td>Broadcast, multicast, and unicast storm control</td>
<td>Disabled. See the “Default Storm Control Configuration” section on page 20-3.</td>
</tr>
<tr>
<td>Port Fast</td>
<td>Disabled. See the “Default Optional Spanning-Tree Configuration” section on page 16-5.</td>
</tr>
<tr>
<td>Auto-MDIX</td>
<td>Enabled.</td>
</tr>
<tr>
<td>Cisco Discovery Protocol (CDP)</td>
<td>Enabled.</td>
</tr>
</tbody>
</table>

Configuring Interface Speed and Duplex Mode

Ethernet interfaces on the switch operate at 10, 100, or 1000 Mb/s or 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 Gigabit Ethernet (10/100/1000-Mb/s) ports and small form-factor pluggable (SFP) module slots supporting SFP modules.

- Speed and Duplex Configuration Guidelines, page 10-14
- Setting the Interface Speed and Duplex Parameters, page 10-15

Speed and Duplex Configuration Guidelines

When configuring an interface speed and duplex mode, note these guidelines:

- You can configure interface speed on Gigabit Ethernet (10/100/1000-Mb/s) ports. You can configure Gigabit Ethernet ports to full-duplex mode or to autonegotiate. You also can configure Gigabit Ethernet ports to half-duplex mode if the speed is 10 or 100 Mb/s. Half-duplex mode is not supported on Gigabit Ethernet ports operating at 1000 Mb/s.
- You cannot configure speed on SFP module ports or on 10 Gigabit Ethernet ports, but you can configure speed to not negotiate (nongotiate) on SFP module ports if connected to a device that does not support autonegotiation.
The exception is when a 1000BASE-T SFP module is in the SFP module slot, you can configure speed as 10, 100, or 1000 Mb/s, or auto, but not as nonegotiate.

On a 100BASE-FX SFP module, you cannot configure the speed as nonegotiate.

- You cannot configure duplex mode on 10 GigabitEthernet ports. The duplex command is not available.
- You cannot configure duplex mode on SFP module ports; they operate in full-duplex mode except in these situations:
  - When a Cisco1000BASE-T SFP module is in the SFP module slot, you can configure duplex mode to auto or full. Half-duplex mode is supported with the auto setting.
  - When a Cisco100BASE-FX SFP module is in the SFP module slot, you can configure duplex mode to half or full. Although the auto keyword is available, it puts the interface in half-duplex mode (the default for this SFP module) because the 100BASE-FX SFP module does not support autonegotiation.
- 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.
- 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>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>interface interface-id</td>
<td>Specify the physical interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>speed {10</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter <strong>10</strong>, <strong>100</strong>, or <strong>1000</strong> to set a specific speed for the interface. The <strong>1000</strong> keyword is available only for 10/100/1000 Mb/s ports or SFP module ports with a 1000BASE-T SFP module.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter <strong>auto</strong> to enable the interface to autonegotiate speed with the connected device. If you use the <strong>10</strong>, <strong>100</strong>, or the <strong>1000</strong> keywords with the <strong>auto</strong> keyword, the port autonegotiates only at the specified speeds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The <strong>nonegotiate</strong> keyword is available but not supported on 10 GigabitEthernet ports. When a Cisco1000BASE-T SFP module is in the SFP module slot, the speed can be configured to <strong>10</strong>, <strong>100</strong>, <strong>1000</strong>, or to <strong>auto</strong>, but not to <strong>nonegotiate</strong>.</td>
</tr>
</tbody>
</table>
Configuring Ethernet Interfaces

Chapter 10      Configuring Interfaces

Configuring Ethernet Interfaces

Configuring Interfaces

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 interface speed to 10 Mb/s and the duplex mode to half:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# speed 10
Switch(config-if)# duplex half
```

This example shows how to set the interface speed to 100 Mb/s on a 10/100/1000 Mb/s port:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# speed 100
```

Configure 802.3x Flow Control

IEEE 802.3x 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 by sending a pause frame to stop sending until the condition clears. 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

Ports can receive, but 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 IEEE 802.3x 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**: IEEE 802.3x 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 IEEE 802.3x 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 IEEE 802.3x flow control on an 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 interface-id</td>
<td>Specify the physical interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>flowcontrol {receive} {on</td>
<td>Configure the IEEE 802.3x flow control mode for the port.</td>
</tr>
<tr>
<td></td>
<td>off</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show interfaces interface-id</td>
<td>Verify the interface IEEE 802.3x flow control settings.</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 IEEE 802.3x flow control, use the **flowcontrol receive off** interface configuration command.

This example shows how to enable IEEE 802.3x flow control on a port:

Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# flowcontrol receive on
Switch(config-if)# end

### Configuring Auto-MDIX on an Interface

When automatic medium-dependent interface crossover (auto-MDIX) is enabled on an interface, the interface 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 interface to **auto** so that the feature operates correctly. Auto-MDIX is supported on all 10/100 and 10/100/1000 Mb/s interfaces and on Cisco 10/100/1000 BASE-T/TX SFP module interfaces. It is not supported on 1000 BASE-SX or -LX SFP module interfaces.

**Table 10-3** shows the link states that result from auto-MDIX settings and correct and incorrect cabling.
### Configuring Ethernet Interfaces

**Beginning in privileged EXEC mode, follow these steps to configure auto-MDIX on an interface:**

1. `configure terminal` - Enter global configuration mode.
2. `interface interface-id` - Specify the physical interface to be configured, and enter interface configuration mode.
3. `speed auto` - Configure the interface to autonegotiate speed with the connected device.
4. `duplex auto` - Configure the interface to autonegotiate duplex mode with the connected device.
5. `mdix auto` - Enable auto-MDIX on the interface.
6. `end` - Return to privileged EXEC mode.
7. `show controllers ethernet-controller interface-id phy` - Verify the operational state of the auto-MDIX feature on the interface.
8. `copy running-config startup-config` - (Optional) Save your entries in the configuration file.

To disable auto-MDIX, use the `no mdix auto` interface configuration command.

This example shows how to enable auto-MDIX on a port:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
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>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 for which you are adding a description, and enter interface configuration mode.</td>
</tr>
</tbody>
</table>
Chapter 10  Configuring Interfaces

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. You cannot delete interface VLAN 1.

  **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 28, “Configuring EtherChannels.”

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 switch port.

- If you try to create an extended-range VLAN, an error message is generated, and the extended-range VLAN is rejected.
Configuring the Interface MTU

You can configure the maximum transmission unit (MTU) size on an interface to determine the packet size that can be received on the interface. Because the switch does not fragment Layer 2 packets, it drops switched Layer 2 packets larger than the packet size supported on the egress interface.

Beginning in privileged EXEC mode, follow these steps to change the MTU size 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 {gigabitethernet} interface-id</td>
<td>Specify the interface to be configured as a Layer 3 interface, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3: no switchport</td>
<td>For physical ports only, enter Layer 3 mode.</td>
</tr>
<tr>
<td>Step 4: ip address ip_address subnet_mask</td>
<td>Configure the IP address and IP subnet.</td>
</tr>
<tr>
<td>Step 5: end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6: show interfaces [interface-id]</td>
<td>Verify the configuration.</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 7: copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</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
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.20.135.21 255.255.255.0
```
This example shows how to set the maximum packet size for a Gigabit Ethernet port to 1800 bytes:

```
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# mtu 1800
Switch(config)# exit
```

### Monitoring and Maintaining the Interfaces

These sections contain interface monitoring and maintenance information:

- Monitoring Interface Status, page 10-21
- Clearing and Resetting Interfaces and Counters, page 10-22
- Shutting Down and Restarting the Interface, page 10-23

### 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 10-4 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, Release 12.2*.

#### Table 10-4 Show Commands for Interfaces

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces [interface-id]</code></td>
<td>Display the status and configuration of all interfaces or a specific interface.</td>
</tr>
<tr>
<td><code>show interfaces interface-id status [err-disabled]</code></td>
<td>Display interface status or a list of interfaces in an error-disabled state.</td>
</tr>
<tr>
<td><code>show interfaces [interface-id] switchport</code></td>
<td>Display administrative and operational status of switching mode. You can use this command to find out if a port is in routing or in switching mode.</td>
</tr>
<tr>
<td><code>show interfaces [interface-id] description</code></td>
<td>Display the description configured on an interface or all interfaces and the interface status.</td>
</tr>
</tbody>
</table>
Table 10-4  Show Commands for Interfaces (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<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 interface [interface-id] stats</td>
<td>Display the input and output packets by the switching path for the interface.</td>
</tr>
</tbody>
</table>
| show interfaces [interface-id] transceiver [detail | dom-supported-list | module number | properties | threshold-table] | Display these physical and operational status about an SFP module:  
  * interface-id--(Optional) Display configuration and status for a specified physical interface.  
  * 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.  
  * dom-supported-list--(Optional) List all supported DoM transceivers.  
  * 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.  
  * properties--(Optional) Display speed, duplex, and inline power settings on an interface  
  * threshold-table--(Optional) Display alarm and warning threshold table |
| show port-type [eni | nni | uni] | Display interface type information for the Cisco ME switch. The only valid type is nni. Other keywords show no output. |
| show running-config interface [interface-id] | Display the running configuration in RAM for the interface. |
| show version | Display the hardware configuration, software version, the names and sources of configuration files, and the boot images. |
| show controllers ethernet-controller interface-id phy | Display the operational state of the auto-MDIX feature on the interface. - Doesn’t seem to show this |

Table 10-5  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 you specify optional arguments that 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 andRestarting 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>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 {vlan vlan-id}</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>shutdown</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>
</tbody>
</table>

Use the `no shutdown` interface configuration command to enable an 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 display.
CHAPTER 11

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 Cisco ME 3800X and ME 3600X switch. It includes information about VLAN membership modes, VLAN configuration modes, and VLAN trunks.

Note

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

- Understanding VLANs, page 11-1
- Creating and Modifying VLANs, page 11-5
- Displaying VLANs, page 11-9
- Configuring VLAN Trunks, page 11-9

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, 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 14, “Configuring STP.”
Figure 11-1 shows an example of VLANs segmented into logically defined networks.

**Figure 11-1  VLANs as 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.

*Note*

The switch does not support VLAN Trunking Protocol (VTP).

Traffic between VLANs must be routed. Switches can route traffic between VLANs by using switch virtual interfaces (SVIs) that are explicitly configured and assigned an IP address. For more information, see the “Switch Virtual Interfaces” section on page 10-4 and the “Configuring Layer 3 Interfaces” section on page 10-19.

This section includes these topics:

- Supported VLANs, page 11-3
- Normal-Range VLANs, page 11-3
- Extended-Range VLANs, page 11-4
- VLAN Port Membership Modes, page 11-4
- UNI VLANs, page 11-4
Supported VLANs

VLANs are identified with a number from 1 to 4094. VLAN IDs 1002 through 1005 are reserved for Token Ring and FDDI VLANs. VLAN IDs greater than 1005 are extended-range VLANs and are not stored in the VLAN database.

Although the switch supports a total of 4094 (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 “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 IEEE 802.1Q trunking for sending VLAN traffic over Ethernet ports.

Normal-Range VLANs

Normal-range VLANs are VLANs with VLAN IDs 1 to 1005. 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.)

Configurations for VLAN IDs 1 to 1005 are written to the file vlan.dat (VLAN database), and you can display them by entering the show vlan privileged EXEC command. The vlan.dat file is stored in flash memory.

Caution

You can cause inconsistency in the VLAN database if you try 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.

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)

Note

The switch supports only Ethernet VLANs. You can configure parameters for FDDI and Token Ring VLANs and view the results in the vlan.dat file, but these parameters are not used.

- 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
Understanding VLANs

- VLAN number to use when translating from one VLAN type to another
- UNI VLAN configuration

For extended-range VLANs, you can configure only VLAN MTU.

**Note**
This chapter 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.

### Extended-Range VLANs

You can create extended-range VLANs (in the range 1006 to 4094) to 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 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.

### VLAN Port Membership Modes

You configure a port to belong to a VLAN by assigning a membership mode that specifies the kind of traffic that the port carries and the number of VLANs to which it can belong. Table 11-1 lists the membership modes and characteristics.

<table>
<thead>
<tr>
<th>Membership Mode</th>
<th>VLAN Membership 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.</td>
</tr>
<tr>
<td></td>
<td>For more information, see the “Assigning Static-Access Ports to a VLAN” section on page 11-8.</td>
</tr>
<tr>
<td>Trunk (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.</td>
</tr>
<tr>
<td></td>
<td>For information about configuring trunk ports, see the “Configuring an Ethernet Interface as a Trunk Port” section on page 11-11.</td>
</tr>
</tbody>
</table>

For more detailed definitions of access and trunk modes and their functions, see Table 11-4 on page 11-10.

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.

### UNI VLANs

The Cisco ME 3800X and 3600X have commands for configuring user network interface (UNI) VLANs to isolate traffic between some ports on a switch.
• UNI isolated VLANs prohibit local switching between UNIs or enhanced network interfaces (ENIs) on a switch.
• UNI community VLANs allow local switching is allowed between these port types.

Because all ports on the ME 3800X and ME 3600X are NNIs, these commands have no effect on the switch.

Creating and Modifying VLANs

You use VLAN configuration mode, accessed by entering the `vlan` global configuration command to create VLANs and to modify some parameters. 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.

These sections contain VLAN configuration information:
• Default Ethernet VLAN Configuration, page 11-5
• VLAN Configuration Guidelines, page 11-6
• Creating or Modifying an Ethernet VLAN, page 11-7
• Assigning Static-Access Ports to a VLAN, page 11-8
• Displaying VLANs, page 11-9

For more efficient management of the MAC address table space available on the switch, you can control which VLANs learn MAC addresses by disabling MAC address learning on specific VLANs. See the “Disabling MAC Address Learning on a VLAN” section on page 5-28 for more information.

Default Ethernet VLAN Configuration

The switch supports only Ethernet interfaces. Table 11-2 shows the default configuration for Ethernet VLANs.

Note
On extended-range VLANs, you can change only the MTU size. All other characteristics must remain at the default conditions.

<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>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>
</tbody>
</table>

Table 11-2 Ethernet VLAN Defaults and Ranges

Note
Extended-range VLANs (VLAN IDs 1006 to 4094) are not saved in the VLAN database.
Chapter 11  Configuring VLANs

Creating and Modifying VLANs

VLAN Configuration Guidelines

- The switch supports 4094 VLANs.
- Normal-range Ethernet VLANs are identified with a number between 1 and 1001. VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs.
- The switch does not support Token Ring or FDDI media. The switch does not forward FDDI, FDDI-Net, TrCRF, or TrBRF traffic.
- VLAN configurations for VLANs 1 to 1005 are always saved in the VLAN database and in the switch running configuration file.
- Configuration options for VLAN IDs 1006 through 4094 (extended-range VLANs) are limited to MTU. Extended-range VLANs are not saved in the VLAN database.
- Spanning Tree Protocol (STP) is enabled by default for ports on all VLANs. 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 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 spanning-tree instance. For more information about MSTP, see Chapter 15, “Configuring MSTP.”
- Although the switch supports a total of 4094 (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.
- In Ethernet virtual connections (EVCs), a bridge domain is similar to a VLAN, except that bridge-domain membership is determined by which service instances have joined (based on encapsulation criteria), while VLAN membership is determined by the VLAN tag in the packet. For more information about bridge domains, see Chapter 12, “Configuring Ethernet Virtual Connections (EVCs).”
Creating or Modifying an Ethernet VLAN

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 that VLAN. You can use the default VLAN configuration (Table 11-2) or enter commands to configure the VLAN.

**Note**
Extended-range VLANs use the default Ethernet VLAN characteristics and the MTU is the only parameter you can change.

For more information about commands available in this mode, see the `vlan` 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.

The configurations of VLAN IDs 1 to 1005 are always saved in the VLAN database (vlan.dat file) with a VLAN number and name and in the switch running configuration file. Extended-range VLANs are not saved in the VLAN database; they are saved in the switch running configuration file. You can save the VLAN configuration in the switch startup configuration file by using the `copy running-config startup-config` privileged EXEC command.

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><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>vlan vlan-id</strong></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>When you create a new VLAN, by default the VLAN is a UNI-ENI isolated VLAN.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>name vlan-name</strong></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>mtu mtu-size</strong></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 vlan</strong> (name vlan-name</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>copy running-config startup config</strong></td>
</tr>
</tbody>
</table>

To delete a VLAN, use the `no vlan vlan-id` global configuration command. You cannot delete VLAN 1 or 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.
Chapter 11 Configuring VLANs

Creating and Modifying VLANs

Assigning Static-Access Ports to a VLAN

You can assign a static-access port to a VLAN.

**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 11-7.)

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><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><code>switchport mode access</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>switchport access vlan vlan-id</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>show running-config interface interface-id</code></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>show interfaces interface-id switchport</code></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>copy running-config startup-config</code></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:

```bash
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabithernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# end
```
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. Table 11-3 lists other privileged EXEC commands for monitoring VLANs.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces [vlan vlan-id]</code></td>
<td>Display characteristics for all interfaces or for the specified VLAN configured on the switch.</td>
</tr>
<tr>
<td><code>show vlan [id vlan-id]</code></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

- **Trunking Overview, page 11-9**
- **Default Layer 2 Ethernet Interface VLAN Configuration, page 11-10**
- **Configuring an Ethernet Interface as a Trunk Port, page 11-11**
- **Configuring Trunk Ports for Load Sharing, page 11-14**

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. The switch supports the IEEE 802.1Q industry-standard trunking encapsulation.

You can configure a trunk on a single Ethernet interface or on an EtherChannel bundle. For more information about EtherChannels, see Chapter 28, “Configuring EtherChannels.”

Ethernet interfaces support different trunking modes (see Table 11-4). You can set an interface as trunking or nontrunking.

- **If you do not intend to trunk across links, use the `switchport mode access` interface configuration command to disable trunking.**
- **To enable trunking, use the `switchport mode trunk` interface configuration command to change the interface to a trunk.**
IEEE 802.1Q Configuration Considerations

The IEEE 802.1Q trunks impose these limitations on the trunking strategy for a network:

- 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. 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 IEEE 802.1Q switch. However, spanning-tree information for each VLAN 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.

- Make sure that 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 IEEE 802.1Q trunk or disable spanning tree on every VLAN in the network. Make sure that your network is loop-free before disabling spanning tree.

Default Layer 2 Ethernet Interface VLAN Configuration

Table 11-5 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>switchport mode access</td>
</tr>
<tr>
<td>Allowed VLAN range</td>
<td>VLANs 1 to 4094</td>
</tr>
<tr>
<td>Default VLAN (for access ports)</td>
<td>VLAN 1</td>
</tr>
<tr>
<td>Native VLAN (for IEEE 802.1Q trunks)</td>
<td>VLAN 1</td>
</tr>
</tbody>
</table>
Configuring an Ethernet Interface as a Trunk Port

- Interaction with EtherChannels, page 11-11
- Defining the Allowed VLANs on a Trunk, page 11-12
- Configuring the Native VLAN for Untagged Traffic, page 11-13
- Configuring the Native VLAN for Untagged Traffic, page 11-13

Interaction with EtherChannels

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 that 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.

Configuring a Trunk Port

Beginning in privileged EXEC mode, follow these steps to configure a port as an IEEE 802.1Q trunk 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>interface interface-id</td>
<td>Specify the port to be configured for trunking, and enter interface</td>
</tr>
<tr>
<td></td>
<td></td>
<td>configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>switchport mode trunk</td>
<td>Configure the interface as a Layer 2 trunk.</td>
</tr>
<tr>
<td>4</td>
<td>switchport access vlan vlan-id</td>
<td>(Optional) Specify the default VLAN, which is used if the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interface stops trunking.</td>
</tr>
<tr>
<td>5</td>
<td>switchport trunk native vlan vlan-id</td>
<td>Specify the native VLAN for IEEE 802.1Q trunks.</td>
</tr>
<tr>
<td>6</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>7</td>
<td>show interfaces interface-id switchport</td>
<td>Display the switchport configuration of the interface in the Administrative Mode field of the display.</td>
</tr>
<tr>
<td>8</td>
<td>show interfaces interface-id trunk</td>
<td>Display the trunk configuration of the interface.</td>
</tr>
<tr>
<td>9</td>
<td>copy running-config startup-config</td>
<td>(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. 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 port as an IEEE 802.1Q trunk with VLAN 33 as the native VLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 33
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. The VLAN 1 minimization feature allows you 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. You do this by removing VLAN 1 from the allowed VLAN list.

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), and Link Aggregation Control Protocol (LACP) 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 is 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 and if the VLAN is in the allowed list for the port.

Beginning in privileged EXEC mode, follow these steps to modify the allowed list of an IEEE 802.1Q trunk:

<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>switchport mode trunk</strong></td>
</tr>
<tr>
<td><strong>Command</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<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 to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><code>switchport mode trunk</code></td>
<td>Configure the interface as a VLAN trunk port.</td>
</tr>
</tbody>
</table>
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 fastethernet0/1
Switch(config-if)# switchport trunk allowed vlan remove 2
Switch(config-if)# end
```

**Note**When using Ethernet Virtual Connections (EVCs), you can configure an Ethernet flow point (EFP) service instance only on trunk ports with no allowed VLANs. Any other configuration is not allowed. See the “Configuring VLANs” chapter for more information.

### Configuring the Native VLAN for Untagged Traffic

A trunk port configured with IEEE 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 IEEE 802.1Q configuration issues, see the “IEEE 802.1Q Configuration Considerations” section on page 11-10.

Beginning in privileged EXEC mode, follow these steps to configure the native VLAN on an IEEE 802.1Q trunk:

<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 Define the interface that is configured as the IEEE 802.1Q trunk, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>switchport trunk native vlan vlan-id Configure the VLAN that is sending and receiving untagged traffic on the trunk port. For vlan-id, the range is 1 to 4094.</td>
</tr>
</tbody>
</table>
Chapter 11 Configuring VLANs

Configuring VLAN Trunks

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 sending 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 that connect 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 the VLAN to which the traffic belongs.

You configure load sharing on trunk ports that have STP enabled 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 14, “Configuring STP.”

#### Load Sharing Using STP Port Priorities

When two ports on the same switch form a loop, the switch uses the STP port priority to decide which port is enabled and which port is in a blocking state. You can set the priorities on a parallel STP 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.
Beginning in privileged EXEC mode on Switch A, follow these steps to configure the network shown in Figure 11-2. Note that you can use any interface numbers; those shown are examples only.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 7  show vlan</td>
<td>Verify that the referenced VLANs exist on Switch A. If not, create the VLANs by entering the VLAN IDs.</td>
</tr>
<tr>
<td>Step 8  configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 9  interface gigabitethernet 0/1</td>
<td>Define the interface to be configured as the Trunk 1 interface, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 10 switchport mode trunk</td>
<td>Configure the port as a trunk port.</td>
</tr>
<tr>
<td>Step 11 spanning-tree vlan 8-10 port-priority 16</td>
<td>Assign the port priority of 16 for VLANs 8 through 10 on Trunk 1.</td>
</tr>
<tr>
<td>Step 12 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 13 show interfaces gigabitethernet 0/1 switchport</td>
<td>Verify the port configuration.</td>
</tr>
<tr>
<td>Step 14 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 15 interface gigabitethernet 0/2</td>
<td>Define the interface to be configured as the Trunk 2 interface, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 16 switchport mode trunk</td>
<td>Configure the port as a trunk port.</td>
</tr>
<tr>
<td>Step 17 spanning-tree vlan 3-6 port-priority 16</td>
<td>Assign the port priority of 16 for VLANs 3 through 6 on Trunk 2.</td>
</tr>
<tr>
<td>Step 18 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 19 show interfaces gigabitethernet 0/2 switchport</td>
<td>Verify the port configuration.</td>
</tr>
<tr>
<td>Step 20 show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 21 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Follow the same steps on Switch B to configure the trunk port for Trunk 1 with a spanning-tree port priority of 16 for VLANs 8 through 10, and the configure trunk port for Trunk 2 with a spanning-tree port priority of 16 for VLANs 3 through 6.

**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 configure terminal</td>
<td>Enter global configuration mode on Switch A.</td>
</tr>
<tr>
<td>Step 2 interface fastethernet0/1</td>
<td>Define the interface to be configured as Trunk port 1, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 switchport mode trunk</td>
<td>Configure the port as a trunk port.</td>
</tr>
<tr>
<td>Step 4 exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 5 interface gigabitethernet0/2</td>
<td>Define the interface to be configured as Trunk port 2, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 6 switchport mode trunk</td>
<td>Configure the port as a trunk port.</td>
</tr>
<tr>
<td>Step 7 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 8 show running-config</td>
<td>Verify your entries. In the display, make sure that the interfaces configured in Steps 2 and 7 are configured as trunk ports.</td>
</tr>
<tr>
<td>Step 9 show vlan</td>
<td>Verify that VLANs 2 through 4 and 8 through 10 are configured on Switch A. If not, create these VLANs.</td>
</tr>
<tr>
<td>Step 10 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 11 interface gigabitethernet0/1</td>
<td>Enter interface configuration mode for Trunk port 2.</td>
</tr>
<tr>
<td>Step 12 spanning-tree vlan 2-4 cost 30</td>
<td>Set the spanning-tree path cost to 30 for VLANs 2 through 4.</td>
</tr>
<tr>
<td>Step 13 exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 14 interface gigabitethernet0/2</td>
<td>Enter interface configuration mode for Trunk port 2.</td>
</tr>
<tr>
<td>Step 15 spanning-tree vlan 8-10 cost 30</td>
<td>Set the spanning-tree path cost to 30 for VLANs 2 through 4.</td>
</tr>
<tr>
<td>Step 16 exit</td>
<td>Return to global configuration mode.</td>
</tr>
</tbody>
</table>
Follow the same steps on Switch B to configure the trunk port for Trunk 1 with a path cost of 30 for VLANs 2 through 4, and configure the trunk port for Trunk 2 with a path cost of 30 for VLANs 8 through 10.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 17</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 18</td>
<td>exit</td>
</tr>
<tr>
<td>Step 19</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 20</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>
An Ethernet Virtual Connection (EVC) is defined by the Metro-Ethernet Forum (MEF) as an association between two or more user network interfaces that identifies a point-to-point or multipoint-to-multipoint path within the service provider network. An EVC is a conceptual service pipe within the service provider network. A bridge domain is a local broadcast domain that is VLAN-ID-agnostic. An Ethernet flow point (EFP) service instance is a logical interface that connects a bridge domain to a physical port or to an EtherChannel group in a switch.

An EVC broadcast domain is determined by a bridge domain and the EFPs that are connected to it. You can connect multiple EFPs to the same bridge domain on the same physical interface, and each EFP can have its own matching criteria and rewrite operation. An incoming frame is matched against EFP matching criteria on the interface, learned on the matching EFP, and forwarded to one or more EFPs in the bridge domain. If there are no matching EFPs, the frame is dropped.

You can use EFPs to configure VLAN translation. For example, if there are two EFPs egressing the same interface, each EFP can have a different VLAN rewrite operation, which is more flexible than the traditional switchport VLAN translation model.

All ME 3800X and ME 3600X switches support EVCs on all licenses.

For detailed information about the commands, see:

- the command reference for this release
- the Cisco IOS Carrier Ethernet Command Reference:
- Master Command Index for Cisco IOS Release 12.4:

This chapter includes:

- Supported EVC Features, page 12-2
- Understanding EVC Features, page 12-3
- Configuring EFPs, page 12-8
- Configuring Other Features on EFPs, page 12-16
- Monitoring EVC, page 12-35
Supported EVC Features

- Service instance—you create, delete, and modify EFP service instances on Ethernet interfaces.
- Encapsulation—you can map traffic to EFPs based on:
  - 802.1Q VLANs (a single VLAN or a list or range of VLANs)
  - 802.1Q tunneling (QinQ) VLANs (a single outer VLAN and a list or range of inner VLANs)
  - Double-tagged frames mapped to EVC based on C-tags (wildcard S-Tags)
  - Cisco QinQ ethertype for S-tags
- Bridge domains—you can configure EFPs as members of a bridge domain (up to 64 EFPs per bridge domain). However when multicast routing is enabled on a bridge domain you can have a maximum of 26 EFPs per bridge domain.
- Rewrite (VLAN translation)
  - Pop symmetric only—the supported rewrite configuration implies egress pushing (adding a tag)
    - `pop 1` removes the outermost tag
    - `pop 2` removes the two outermost tags
    - `pop symmetric` adds a tag (or 2 tags for `pop 2 symmetric`) on egress for a push operation
  - QinQ with rewrite
  - Ingress rewrite is not supported
- EVC forwarding
- MAC address learning and aging
- EVCs on EtherChannels
- Hairpinning
- Split horizon
- Layer 2 protocol tunneling and QinQ
- EVC MAC address security
- Bridging between switchports and EFPs
- MSTP (MST on EVC bridge domain)
- EFP statistics (packets and bytes)
- QoS aware EVC/EFP per service instance

These Layer 2 port-based features can run with EVC configured on the port:

- PAGP
- LACP
- UDLD
- LLDP
- CDP
- MSTP
Understanding EVC Features

- Ethernet Virtual Connections, page 12-3
- Service Instances and EFPs, page 12-3
- Encapsulation, page 12-4
- Bridge Domains, page 12-6
- Configuring Other Features on EFPs, page 12-16
- Rewrite Operations, page 12-7

Ethernet Virtual Connections

You use the `ethernet evc evc-id` global configuration command to create an Ethernet virtual connection (EVC). The `evc-id` or name is a text string from 1 to 100 bytes. Entering this command puts the device into service configuration mode (config-srv) where you configure all parameters that are common to an EVC.

In this mode you can enter these commands:

- `default`—Sets a command to its defaults
- `exit`—Exits EVC configuration mode
- `no`—Negates a command or sets its defaults
- `oam`—Specifies the OAM Protocol
- `uni`—Configures a count UNI under EVC

Service Instances and EFPs

Configuring a service instance on a Layer 2 port or EtherChannel creates a pseudoport or Ethernet flow point (EFP) on which you configure EVC features. Each service instance has a unique number per interface, but you can use the same number on different interfaces because service instances on different ports are not related.

If you have defined an EVC by entering the `ethernet evc evc-id` global configuration command, you can associate the EVC with the service instance (optional). There is no default behavior for a service instance. You can configure a service instance only on trunk ports with no allowed VLANs. Any other configuration is not allowed. After you have configured a service instance on an interface, switchport commands are not allowed on the interface. You can also configure a service instance on an EtherChannel group.

Use the `service instance number ethernet [name]` interface configuration command to create an EFP on a Layer 2 interface or EtherChannel and to enter service instance configuration mode. You use service instance configuration mode to configure all management and control date plane attributes and parameters that apply to the service instance on a per-interface basis.

- The `service instance number` is the EFP identifier, an integer from 1 to 4000.
- The optional `ethernet name` is the name of a previously configured EVC. You do not need to enter an EVC `name`, but you must enter `ethernet`. Different EFPs can share the same name when they correspond to the same EVC. EFPs are tied to a global EVC through the common name.
When you enter service instance configuration mode, you can configure these options:

- **default**—Sets a command to its defaults
- **description**—Adds a service instance specific description
- **encapsulation**—Configures Ethernet frame match criteria
- **errdisable**—Configures error disable
- **ethernet**—Configures Ethernet-lmi parameters
- **exit**—Exits from service instance configuration mode
- **l2protocol**—Configures Layer 2 control protocol processing
- **mac**—Commands for MAC address-based features
- **no**—Negates a command or sets its defaults
- **service-policy**—Attaches a policy-map to an EFP
- **shutdown**—Takes the service instance out of service

Enter the `[no] shutdown` service-instance configuration mode to shut down or bring up a service instance.

On a Layer 2 port with no service instance configured, multiple `switchport` commands are available (access, backup, block, host, mode, and trunk). When one or more service instances are configured on a Layer 2 port, no `switchport` commands are accepted on that interface.

**Encapsulation**

Encapsulation defines the matching criteria that maps a VLAN, a range of VLANs, cost of service (CoS) bits, Ethertype, or a combination of these to a service instance. You configure encapsulation in service instance configuration mode. You must configure one encapsulation command per EFP (service instance).

Use the `encapsulation` service-instance configuration mode command to set encapsulation criteria. Different types of encapsulations are default, dot1q, priority-tagged and untagged. Valid Ethertypes (type) are ipv4, ipv6, pppoe-all, pppoe-discovery, and pppoe-session.

Encapsulation classification options also include:

- outer tag VLAN
- outer tag CoS
- inner tag VLAN
- inner tag CoS
- payload ethertype—any ethertype tag after the VLAN tag

After you have entered an encapsulation method, these keyword options are available in service instance configuration mode:

- **bridge-domain**—Configures a bridge domain
- **rewrite**—Configures Ethernet rewrite criteria
If a packet entering or leaving a port does not match any of the encapsulations on that port, the packet is dropped, resulting in filtering on both ingress and egress. The encapsulation must match the packet on the wire to determine filtering criteria. On the wire refers to packets ingressing the switch before any rewrites and to packets egressing the switch after all rewrites.
Chapter 12  Configuring Ethernet Virtual Connections (EVCs)

Understanding EVC Features

Note

The switch does not allow overlapping encapsulation configurations. See the “Examples of Unsupported Configurations” section on page 12-14.

Bridge Domains

A service instance must be attached to a bridge domain. Flooding and communication behavior of a bridge domain is similar to that of a VLAN domain. Bridge-domain membership is determined by which service instances have joined it (based on encapsulation criteria), while VLAN domain membership is determined by the VLAN tag in the packet.

Note

You must configure encapsulation before you can configure the bridge domain.

Use the bridge-domain bridge-id service-instance configuration mode command to bind the EFP to a bridge domain instance. The bridge-id is the identifier for the bridge domain instance, an integer from 1 to 8000.

Note

Egress policies will not work if the egress EFPs bridge identifier is greater than 4095.

The switches support up to 8000 bridge domains on the highest end platform and license.

Split-Horizon

The split-horizon feature allows service instances in a bridge domain to join groups. Service instances in the same bridge domain and split-horizon group cannot forward data between each other, but can forward data between other service instances that are in the same bridge domain, but not in the same split-horizon group.

Service instances do not have to be in a split-horizon group. If a service instance does not belong to a group, it can send and receive from all ports within the bridge domain. A service instance cannot join more than one split-horizon group.

Enter the bridge-domain bridge-id split-horizon group group_id service-instance configuration mode command to configure a split-horizon group. The group_id is an integer from 0 to 2. All members of the bridge-domain that are configured with the same group_id are part of the same split-horizon group. EFPs that are not configured with an explicit group_id do not belong to any group.

You can configure no more than 64 service instances per bridge domain. When a bridge domain contains a service instance that is part of a split-horizon group, this decreases the number of service instances allowed to be configured in that split-horizon group. The switch supports up to three split-horizon groups plus the default (no group).

In Table 12-2, the left column means that a bridge domain belongs to a service instance that is part of the indicated split horizon group. Therefore, if a service instance joins split-horizon group 2, it can have no more than 16 members in split horizon group 2 in the same bridge domain. We recommend that you add split horizon groups in numerical order to maximize the number of service instances that can belong to a group.
### Rewrite Operations

You can use the `rewrite` command to modify packet VLAN tags. You can use this command to emulate traditional 802.1Q tagging, where packets enter a switch on the native VLAN and VLAN tagging properties are added on egress. You can also use the `rewrite` command to facilitate VLAN translation and QinQ.

The ME 3800X and ME 3600X switches support only these `rewrite` commands.

- `rewrite ingress tag pop 1 symmetric`
- `rewrite ingress tag pop 2 symmetric`

Enter the `rewrite ingress tag pop {1 | 2} symmetric` service-instance configuration mode command to specify the encapsulation adjustment to be performed on the frame ingress to the EFP. Entering `pop 1` pops (removes) the outermost tag; entering `pop 2` removes two outermost tags.

**Note**

When you enter the `symmetric` keyword, the egress counterpart performs the inverse action and pushes (adds) the encapsulation VLAN. You can use the `symmetric` keyword only with ingress rewrites and only when single VLANs are configured in encapsulation. If you configure a list of VLANs or a VLAN range or `encapsulation default` or `encapsulation any`, the `symmetric` keyword is not accepted for rewrite operations.

The switch does not support `rewrite` commands for `ingress push` and `translate` in this release. However, you can use the `rewrite ingress tag pop symmetric` command to achieve translation. Possible translation combinations are 1-to-1, 1-to-2, 2-to-1, and 2-to-2. When forwarding to or from a Layer 2 port, you cannot achieve 2-to-2 translation because a Layer 2 port is implicitly defined to be `rewrite ingress tag pop 1 symmetric`.

The switch does not support egress rewrite operations beyond the second VLAN that a packet carries into a switch. Because of the egress rewrite limitation, if an EFP has a `pop 2 rewrite` operation at ingress, no other EFP in the same bridge domain can have a rewrite operation. See the “Global Rewrite Operation Limitation on a Switch” section on page 12-15.
Configuring EFPs

- Default EVC Configuration, page 12-8
- Configuration Guidelines, page 12-8
- Creating Service Instances, page 12-9
- Configuration Examples, page 12-10
- Examples of Unsupported Configurations, page 12-14

Default EVC Configuration

No EFPs are configured. No service instances or bridge domains are configured.

Configuration Guidelines

- You can configure 4000 bridge domains on the ME 3600X switch.
- On the ME 3800X switch, the number of bridge domains that you can configure depends on the license that is installed on the switch:
  - The metro services licenses support 4000 bridge domains.
  - The metro IP services licenses support 2000 bridge domains.
  - The metro aggregation services license supports 4000 bridge domain and the scaled version supports 8000 bridge domains.
- All licenses support a maximum of 64 EFPs per bridge domain.
- On ME 3600X you can configure the following number of EFPs and cross connects per port:
  - 4000 service instances per port
  - 512 EFP xconnects per port
  - 512 overall on device
- On ME 3800X you can configure the following number of EFPs and cross connects per port:
  - 4000 service instances per port
  - 4000 EFP xconnects per port
  - 8000 overall on device
- Layer 2 protocol tunneling is not supported on cross-connect EFPs.
- You can configure a service instance only on trunk ports with no allowed VLANs. Any other configuration is not allowed. To configure a service instance on an interface, these commands are prerequisites:
  
  Switch (config)# interface gigabitethernet0/2  
  Switch (config-if)# switchport mode trunk  
  Switch (config-if)# switchport trunk allowed vlan none
- After you have configured a service instance on an interface, switchport commands are not allowed on that interface.
- You must configure encapsulation on a service instance before configuring bridge domain.
Chapter 12 Configuring Ethernet Virtual Connections (EVCs)

Configuring EFPs

- The native VLAN ID specified in `switchport trunk native vlan-id` is not used by EVC.
- ISL trunk encapsulation is not supported.
- When an EFP encapsulation is the default (matching or allowing all ingress frames), you cannot configure any other encapsulation on an EFP on the same port and bridge-domain as the default encapsulation. There can be only one default encapsulation per port.
- The switch does not support overlapping configurations on the same interface and same bridge domain. If you have configured a VLAN range encapsulation, or encapsulation default, or encapsulation any on service instance 1, you cannot configure any other encapsulations that also match previous encapsulations in the same interface and bridge domain. See the “Examples of Unsupported Configurations” section on page 12-14.

Creating Service Instances

Beginning in privileged EXEC mode, follow these steps to create an EFP service instance:

<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> Specify the port to attach to the policy map, and enter interface configuration mode. Valid interfaces are physical ports.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>switchport mode trunk</code> Configure the interface as a trunk port, required for EFP configuration.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>switchport trunk allowed vlan none</code> Configure the trunk port to have no allowed VLANs.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>service instance number ethernet [name]</code> Configure an EFP (service instance) and enter service instance configuration mode.</td>
</tr>
<tr>
<td></td>
<td>- The <code>number</code> is the EFP identifier, an integer from 1 to 4000.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) <code>ethernet name</code> is the name of a previously configured EVC. You do not need to use an EVC name in a service instance.</td>
</tr>
<tr>
<td>Step 6</td>
<td>`encapsulation {default</td>
</tr>
<tr>
<td></td>
<td>- <code>default</code>—Configure to match all unmatched packets.</td>
</tr>
<tr>
<td></td>
<td>- <code>dot1q</code>—Configure 802.1Q encapsulation. See Table 12-1 for details about options for this keyword.</td>
</tr>
<tr>
<td></td>
<td>- <code>priority-tagged</code>—Specify priority-tagged frames, VLAN-ID 0 and CoS value of 0 to 7.</td>
</tr>
<tr>
<td></td>
<td>- <code>untagged</code>—Map to untagged VLANs. Only one EFP per port can have untagged encapsulation.</td>
</tr>
</tbody>
</table>
Chapter 12  Configuring Ethernet Virtual Connections (EVCs)

Configuring EFPs

Use the `no` forms of the commands to remove the service instance, encapsulation type, or bridge domain or to disable the rewrite operation.

### Configuration Examples

#### Configuring a Service Instance

```bash
Switch (config)# interface gigabitethernet0/1
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan none
Switch (config-if)# service instance 22 Ethernet
Switch (config-if-srv)# encapsulation dot1q 10
Switch (config-if-srv)# bridge-domain
```

#### Encapsulation Using a VLAN Range

```bash
Switch (config)# interface gigabitethernet0/1
Switch (config-if)# service instance 22 Ethernet
Switch (config-if-srv)# encapsulation dot1q 22-44
Switch (config-if-srv)# bridge-domain
```
Two Service Instances Joining the Same Bridge Domain

In this example, service instance 1 on interfaces Gigabit Ethernet 0/1 and 0/2 can bridge between each other.

Switch (config)# interface gigabitethernet0/1
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation dot1q 10
Switch (config-if-srv)# bridge-domain 10

Switch (config)# interface gigabitethernet0/2
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation dot1q 10
Switch (config-if-srv)# bridge-domain 10

Bridge Domains and VLAN Encapsulation

Unlike VLANs, the bridge-domain number does not need to match the VLAN encapsulation number.

Switch (config)# interface gigabitethernet0/1
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation dot1q 10
Switch (config-if-srv)# bridge-domain 8000

Switch (config)# interface gigabitethernet0/2
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation dot1q 10
Switch (config-if-srv)# bridge-domain 8000

However, when encapsulations do not match in the same bridge domain, traffic cannot be forwarded. In this example, the service instances on Gigabit Ethernet 0/1 and 0/2 can not forward between each other, since the encapsulations don’t match (filtering criteria). However, you can use the rewrite command to allow communication between these two.

Switch (config)# interface gigabitethernet0/1
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation dot1q 10
Switch (config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch (config-if-srv)# bridge-domain 8000

Rewrite

In this example, a packet that matches the encapsulation will have one tag removed (popped off). The symmetric keyword allows the reverse direction to have the inverse action: a packet that egresses out this service instance will have the encapsulation (VLAN 10) added (pushed on).

Switch (config)# interface gigabitethernet0/1
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation dot1q 10
Switch (config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch (config-if-srv)# bridge-domain 8000
Split Horizon

In this example, service instances 1 and 2 cannot forward and receive packets from each other. Service instance 3 can forward traffic to any service instance in bridge domain 8000 since no other service instance in bridge domain 8000 is in split-horizon group 2. Service instance 4 can forward traffic to any service instance in bridge domain 8000 since it has not joined any split-horizon groups.

Switch (config)# interface gigabitethernet0/1
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation dot1q 10
Switch (config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch (config-if-srv)# bridge-domain 8000 split-horizon group 1
Switch (config-if-srv)# exit
Switch (config-if)# service instance 2 Ethernet
Switch (config-if-srv)# encapsulation dot1q 99
Switch (config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch (config-if-srv)# bridge-domain 8000 split-horizon group 1

Switch (config)# interface gigabitethernet0/2
Switch (config-if)# service instance 3 Ethernet
Switch (config-if-srv)# encapsulation dot1q 10
Switch (config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch (config-if-srv)# bridge-domain 8000 split-horizon group 2
Switch (config-if-srv)# exit
Switch (config-if)# service instance 4 Ethernet
Switch (config-if-srv)# encapsulation dot1q 99
Switch (config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch (config-if-srv)# bridge-domain 8000

Hairpinning

The switch supports hairpinning, which refers to traffic ingressing and egressing same interface. To achieve hairpinning, configure two EFPs in the same bridge domain on the same physical interface, as in this example.

Switch (config)# interface gigabitethernet0/2
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation dot1q 10
Switch (config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch (config-if-srv)# bridge-domain 5000
Switch (config-if-srv)# exit
Switch (config-if)# service instance 2 Ethernet
Switch (config-if-srv)# encapsulation dot1q 20
Switch (config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch (config-if-srv)# bridge-domain 5000

Egress Filtering

In EVC switching, egress filtering is performed before the frame is sent on the egress EFP. Egress filtering ensures that when a frame is sent, it conforms to the matching criteria of the service instance applied on the ingress direction. EFP does not require egress filtering if the number of pops is the same as the number of VLANs specified in the encapsulation command.

Note

Specifying the cos keyword in the encapsulation command is relevant only in the ingress direction. For egress filtering, cos is ignored.

For example, consider the following configuration.
Switch (config)# interface gigabitethernet0/1
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation dot1q 20
Switch (config-if-srv)# bridge-domain 19

Switch (config)# interface gigabitethernet0/2
Switch (config-if)# service instance 2 Ethernet
Switch (config-if-srv)# encapsulation dot1q 30
Switch (config-if-srv)# bridge-domain 19

Switch (config)# interface gigabitethernet0/3
Switch (config-if)# service instance 3 Ethernet
Switch (config-if-srv)# encapsulation dot1q 10 second-dot1q 20
Switch (config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch (config-if-srv)# bridge-domain 19

If a packet with VLAN tag 10 or 20 is received on Gigabit Ethernet 0/3, the ingress logical port would be service instance 3. For the frame to be forwarded on a service instance, the egress frame must match the encapsulation defined on that service instance after the rewrite is done. Service instance 1 checks for outermost VLAN 20; service instance 2 checks for VLAN 30. In this example, the frame with VLAN tags 10 and 20 can be sent to service instance 1 but not to service instance 2.

**l2protocol Forward Option**

The l2protocol forward option causes the EVC interface to flood the untagged/tagged BPDU packets on:

- another trunk interface on the same VLAN/BD
- SVI or VFI Pseudowire
- EVCs on the same BD

This is an example how to configure the l2protocol forward option:

```plaintext
interface GigabitEthernet0/9
switchport trunk allowed vlan none
switchport mode trunk
ethernet uni id PRAV-PE2
service instance 1 ethernet
  encapsulation dot1q 500
  l2protocol forward cdp
  bridge-domain 500
!

service instance 10 ethernet xcon
  encapsulation dot1q 100
  l2protocol forward cdp
  xconnect 4.3.2.1 12 encapsulation mpls
```

Examples of Unsupported Configurations

Overlapping Encapsulation

The switch does not allow overlapping encapsulation. Overlapping encapsulation configuration occurs when two EFPS are configured on the same port and the same bridge domain and the set of encapsulations on one EFP is a subset of the encapsulations on the other EFP.

These are examples of overlapping encapsulation:

Example 1

Service instance 2 configuration is rejected because the service instance 1 encapsulation default is a superset of service instance 2 encapsulation dot1q 10.

Switch (config)# interface gigabitethernet 0/1
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport mode allowed vlan none
Switch (config-if)# service instance 1 ethernet
Switch (config-if-srv)# encapsulation default
Switch (config-if-srv)# bridge-domain 10
Switch (config-if-srv)# exit
Switch (config-if)# service instance 2 ethernet
Switch (config-if-srv)# encapsulation dot1q 10
Switch (config-if-srv)# bridge-domain 10

Example 2

Service instance 2 configuration is rejected because service instance 1 encapsulation dot1q any is superset of service instance 2 encapsulation dot1q 10.

Switch (config)# interface gigabitethernet 0/1
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport mode allowed vlan none
Switch (config-if)# service instance 1 ethernet
Switch (config-if-srv)# encapsulation dot1q any
Switch (config-if-srv)# bridge-domain 10
Switch (config-if-srv)# exit
Switch (config-if)# service instance 2 ethernet
Switch (config-if-srv)# encapsulation dot1q 10
Switch (config-if-srv)# bridge-domain 10

Example 3

Service instance 2 configuration is rejected. Both service instances have the same dot1q vlan 10 encapsulation, but matching cos 3 in service instance 1 is subset of service instance 2 cos match all (the default when not specified). Matching etype ipv4 in service instance 2 is a subset of service instance 1 etype match all (the default when not specified).

Switch (config)# interface gigabitethernet 0/1
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport mode allowed vlan none
Switch (config-if)# service instance 1 ethernet
Switch (config-if-srv)# encapsulation dot1q 10 cos 3
Switch (config-if-srv)# bridge-domain 10
Switch (config-if-srv)# exit
Switch (config-if)# service instance 2 ethernet
Switch (config-if-srv)# encapsulation dot1q 10 etype ipv4
Switch (config-if-srv)# bridge-domain 10
Global Rewrite Operation Limitation on a Switch

The switch does not support egress rewrite operations beyond the second VLAN that a packet carries into a switch. Because of the egress rewrite limitation, if an EFP has a **pop 2 rewrite** operation at ingress, no other EFP in the same bridge domain can have a rewrite operation.

In these examples, service instance 1 and the switchport characteristics are configured prior to service instance 2. In the examples, **dot1q 30** identifies a third VLAN to be parsed.

**Example 1**

Service instance 1 pops two tags at ingress, and service instance 2 does not have rewrite (push) operation at egress. The configuration for service instance 2 is rejected because it is configuring a match on the third VLAN of the packet bridged from service instance 1 to dot1q VLAN encapsulation of service instance 2.

```
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation dot1q 10 second-dot1q 20
Switch (config-if-srv)# rewrite ingress tag pop 2 symmetric
Switch (config-if-srv)# bridge-domain 2
Switch (config-if-srv)# exit
Switch (config-if)# service instance 2 Ethernet
Switch (config-if-srv)# encapsulation dot1q 30
Switch (config-if-srv)# bridge-domain 2
```

**Example 2**

Service instance 1 pops two tags at ingress, and service instance 2 pushes only the outermost VLAN. The service instance 2 configuration is rejected since it configures a match on the third VLAN of the packet bridged from service instance 1 to the **second-dot1q 30** encapsulation of service instance 2.

```
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation dot1q 10 second-dot1q 20
Switch (config-if-srv)# rewrite ingress tag pop 2 symmetric
Switch (config-if-srv)# bridge-domain 2
Switch (config-if-srv)# exit
Switch (config-if)# service instance 2 Ethernet
Switch (config-if-srv)# encapsulation dot1q 15 second-dot1q 30
Switch (config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch (config-if-srv)# bridge-domain 2
```

**Example 3**

Service instance 1 pops only one tag, and service instance 2 needs to parse the second and third VLANs. Service instance 2 configuration is rejected since it needs to match on the third VLAN of the packet bridged from service instance 1 to the **second-dot1q 30** encapsulation of service instance 2.

```
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation dot1q 10 second-dot1q 20
Switch (config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch (config-if-srv)# bridge-domain 2
Switch (config-if-srv)# exit
Switch (config-if)# service instance 2 Ethernet
Switch (config-if-srv)# encapsulation dot1q 15 second-dot1q 30
Switch (config-if-srv)# bridge-domain 2
```
Example 4

The switchport pops the outermost VLAN implicitly, and service instance 2 needs to parse the second and third VLANs. In this case, the service instance 2 configuration is rejected because it needs to match on the third VLAN of the packet bridged from the switchport to the second-dot1q encapsulation of service instance 2.

```
Switch (config)# interface gigabitethernet 0/1
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan 2

Switch (config)# interface gigabitethernet 0/2
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan none
Switch (config-if)# service instance 2 Ethernet
Switch (config-if-srv)# encapsulation dot1q 20 second-dot1q 30
Switch (config-if-srv)# bridge-domain 2
```

**Note**

In all of these examples, if service instance 2 was configured before service instance 1, the configuration for service instance 1 would be rejected.

**Restricted number of tags supported on EVC and switchport**

Where the EVC matches two tags and there is no rewrite, the configuration is rejected when a second switch port is configured on that VLAN.

A configuration like the example shown below is not supported as the gigabitethernet 2 will be active on vlan 100

```
Switch (config)# interface gigabitethernet 0/1
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan none
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation dot1q 100 second-dot1q 101
Switch (config-if-srv)# bridge-domain 100

Switch (config)# interface gigabitethernet 0/2
Switch (config-if)# switchport mode trunk
```

**Configuring Other Features on EFPs**

- EFPs and EtherChannels, page 12-17
- EFPs and Layer 2 Protocols, page 12-17
- MAC Address Forwarding, Learning and Aging on EFPs, page 12-17
- Configuring IEEE 802.1Q Tunneling and Layer 2 Protocol Tunneling Using EFPs, page 12-18
- EFPs and Ethernet over Multiprotocol Layer Switching (EoMPLS), page 12-25
- Bridge Domain Routing, page 12-26
- EVC and Switchports, page 12-27
- EFPs and MSTP, page 12-31
- L3 Unicast and Multicast Routing on a Bridge Domain with Multiple EFPs, page 12-31
- Cross-Connect on EFP Interfaces, page 12-33
EFPs and EtherChannels

You can configure EFP service instances on EtherChannel port channels, but EtherChannels are not supported on ports configured with service instances. Load-balancing on port channels is based on the MAC address or IP address of the traffic flow on the EtherChannel interface.

This example configures a service instance on an EtherChannel port channel, which is required for the port channel to be operational. Configuration on the ports in the port channel are independent from the service instance configuration.

Switch (config)# interface port-channel 4
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan none
Switch (config-if)# service instance 1 ethernet
Switch (config-if-srv)# encapsulation untagged
Switch (config-if-srv)# bridge-domain {native vlan}
Switch (config-if-srv)# l2protocol peer {lacp | pagp}

EFPs and Layer 2 Protocols

For Layer 2 protocols (CDP, UDLD, LLDP, MSTP, LACP, PAgP, VTP, and DTP) to peer with a neighbor on a port that has an EFP service instance configured, you need to enter the l2 protocol peer protocol service-instance configuration command on the service instance.

This example shows how to configure CDP to peer with a neighbor on a service instance:

Switch (config)# interface gigabitethernet0/1
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan none
Switch (config-if)# service instance 1 ethernet
Switch (config-if-srv)# encapsulation untagged
Switch (config-if-srv)# l2protocol peer cdp
Switch (config-if-srv)# bridge-domain 10
Switch (config-if-srv)# end

MAC Address Forwarding, Learning and Aging on EFPs

- Layer 2 forwarding is based on the bridge domain ID and the destination MAC address. The frame is forwarded to an EFP if the binding between the bridge domain, destination MAC address, and EFP is known. Otherwise, the frame is flooded to all the EFPs or ports in the bridge domain.

- MAC address learning is based on bridge domain ID, source MAC addresses, and logical port number. MAC addresses are managed per bridge domain when the incoming packet is examined and matched against the EFPs configured on the interface. If there is no EFP configured, the bridge domain ID equal to the outer-most VLAN tag is used as forwarding and learning look-up key. For native VLAN frames, the bridge domain equal to the access VLAN configured in the interface is used.

If there is no matching entry in the Layer 2 forwarding table for the ingress frame, the frame is flooded to all the ports within the bridge domain. Flooding within the bridge domain occurs for unknown unicast, unknown multicast, and broadcast.
• Dynamic addresses are addresses learned from the source MAC address when the frame enters the switch. All unknown source MAC addresses are sent to the CPU along with ingress logical port number and bridge domain ID for learning. Once the MAC address is learned, the subsequent frame with the destination MAC address is forwarded to the learned port. When a MAC address moves to a different port, the Layer 2 forwarding entry is updated with the corresponding port.

You can disable learning on a bridge domain by entering the `no mac address-table learning bridge-domain bridge-id` global configuration command. To save Layer 2 forwarding entries, you can disable MAC learning when there are only two EFPs connected to a bridge domain.

• Dynamic addresses are aged out if there is no frame from the host with the MAC address. If the aged-out frame is received by the switch, it is flooded to the EFPs in the bridge domain and the Layer 2 forwarding entry is created again. The default for aging dynamic addresses is 5 minutes. However, when PVST+ undergoes a topology change, the aging time is reduced to the `forward-delay` time configured by the spanning tree. The aging time reverts back to the last configured value when the topology change expires.

You can configure dynamic address aging time per VLAN by entering the `mac address-table aging time [0 | 10-1000000] bridge-domain bridge-id`. The range is in seconds. An aging time of 0 means that the address aging is disabled.

• MAC address movement is detected when the host moves from one port to another. If a host moves to another port or EFP, the learning lookup for the installed entry fails because the ingress logical port number does not match and a new learning cache entry is created. The detection of MAC address movement is disabled for static MAC addresses where the forwarding behavior is configured by the user.

• Static MAC addresses cannot be configured on EFPs. Static MAC addresses are only supported on switch ports.

Configuring IEEE 802.1Q Tunneling and Layer 2 Protocol Tunneling Using EFPs

Tunneling is a feature used by service providers whose networks carry traffic of multiple customers and who are required to maintain the VLAN and Layer 2 protocol configurations of each customer without impacting the traffic of other customers. The ME 3800X and ME 3600X switches use EFPs to support QinQ and Layer 2 protocol tunneling.

802.1Q Tunneling (QinQ)

Service provider 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 802.1Q specification.

Using the EVCs, service providers can encapsulate packets that enter the service-provider network with multiple customer VLAN IDs (C-VLANs) and a single 0x8100 Ethertype VLAN tag with a service provider VLAN (S-VLAN). Within the service provider network, packets are switched based on the S-VLAN. When the packets egress the service provider network onto the customer network, the S-VLAN tag is decapsulated and the original customer packet is restored.

Figure 12-1 shows the tag structures of the double-tagged packets.
In Figure 12-2, Customer A was assigned VLAN 30, and Customer B was assigned VLAN 40. Packets entering the edge switches with 802.1Q tags are double-tagged when they enter the service-provider network, with the outer tag containing VLAN ID 30 or 40, respectively, 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. 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 port, the original VLAN numbers on the customer's network are recovered.
You can use EFPs to configure 802.1Q tunneling in two ways:

**Method 1**

In this example, for Customer A, interface Gigabit Ethernet 0/1 is the customer-facing port, and Gigabit Ethernet 0/2 is a trunk port facing the service provider network. For Customer B, Gigabit Ethernet 0/3 is the customer-facing port, and Gigabit Ethernet 0/4 is the trunk port facing the service provider network.

**Customer A**

```console
Switch (config)# interface gigabitethernet0/1
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation dot1q 1-100
Switch (config-if-srv)# bridge-domain 5000
```

```console
Switch (config)# interface gigabitethernet0/2
Switch (config-if)# service instance 2 Ethernet
Switch (config-if-srv)# encapsulation dot1q 30
Switch (config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch (config-if-srv)# bridge-domain 5000
```

For Customer A, service instance 1 on Gigabit Ethernet port 0/1 is configured with the VLAN encapsulations used by the customer: C-VLANs 1–100. These are forwarded on bridge-domain 5000. The service provider facing port is configured with a service instance on the same bridge-domain and with an `encapsulation dot1q` command matching the S-VLAN. The `rewrite ingress tag pop 1 symmetric` command also implies a push of the configured encapsulation on egress packets. Therefore, the original packets with VLAN tags between 1 and 100 are encapsulated with another S-VLAN (VLAN 30) tag when exiting Gigabit Ethernet port 0/2.

Similarly, for double-tagged (S-VLAN = 30, C-VLAN = 1–100) packets coming from the provider network, the `rewrite ingress tag pop 1 symmetric` command causes the outer S-VLAN tag to be popped and the original C-VLAN tagged frame to be forwarded over bridge-domain 5000 out to Gigabit Ethernet port 0/1.
The same scenario applies to Customer B.

Customer B

```plaintext
Switch (config)# interface gigabitethernet0/3
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation dot1q 1-200
Switch (config-if-srv)# bridge-domain 5000

Switch (config)# interface gigabitethernet0/4
Switch (config-if)# service instance 2 Ethernet
Switch (config-if-srv)# encapsulation dot1q 40
Switch (config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch (config-if-srv)# bridge-domain 5000
```

**Method 2**

QinQ is also supported when sending packets between an EFP and a switchport trunk, because the switchport trunk is implicitly defined as rewrite ingress tag pop 1 symmetric. The same external behavior as Method 1 can be achieved with this configuration:

Customer A

```plaintext
Switch (config)# interface gigabitethernet0/1
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation dot1q 1-100
Switch (config-if-srv)# bridge-domain 30

Switch (config)# interface gigabitethernet0/2
Switch (config-if)# switchport mode trunk
```

Again, service instance 1 on Gigabit Ethernet port 0/1 is configured with the VLAN encapsulations used by the customer: C-VLANs 1–100. These are forwarded on bridge-domain 30. The service provider facing port is configured as a trunk port. The trunk port implicitly pushes a tag matching the bridge-domain that the packet is forwarded on (in this case S-VLAN 30).

---

**Note**

The bridge-domain used must be allowed on the trunk port. This means it must be in the range 1 to 4094 and must be allowed on that trunk port (`switchport trunk allowed vlan` must include 30).

For double tagged (S-VLAN = 30, C-VLAN = 1 to 100) packets coming in from the provider network, the trunk port implicitly pops the outer S-VLAN (30) and forwards the packet on that bridge-domain.

Customer B

```plaintext
Switch (config)# interface gigabitethernet0/3
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation dot1q 1-200
Switch (config-if-srv)# bridge-domain 40

Switch (config)# interface gigabitethernet0/4
Switch (config-if)# switchport mode trunk
```

For information about the effect on cost of service (CoS) for different EFT tagging operations, see the “CoS Mapping” section on page 27-9 in Chapter 27, “Configuring Quality of Service (QoS).”

**VLAN Translation Example Configurations**

- To configure untagged to tagged packets, for implicit push on ingress and pop on the ingress, configure the ingress port as:

  ```plaintext
  Switch (config)# interface gigabitethernet0/1
  ```
Switch (config-if)# switchport access vlan 10
or
Switch (config)# interface gigabitethernet0/1
Switch (config-if)# switchport trunk native vlan 10
Switch (config-if)# switchport mode trunk

Configure the egress port with switchport mode trunk.

- For 1-to-1 VLAN translation (EFP to EFP), ingress port configuration:

  Switch (config)# interface gigabitethernet0/1
  Switch (config-if)# switchport trunk allowed vlan none
  Switch (config-if)# switchport mode trunk
  Switch (config-if)# service instance 10 Ethernet
  Switch (config-if-srv)# encapsulation dot1q 10
  Switch (config-if-srv)# rewrite ingress tag pop 1 symmetric
  Switch (config-if-srv)# bridge-domain 10

  Egress port configuration:

  Switch (config)# interface gigabitethernet0/2
  Switch (config-if)# switchport trunk allowed vlan none
  Switch (config-if)# switchport mode trunk
  Switch (config-if)# service instance 10 Ethernet
  Switch (config-if-srv)# encapsulation dot1q 20
  Switch (config-if-srv)# rewrite ingress tag pop 1 symmetric
  Switch (config-if-srv)# bridge-domain 10

- For 1-to-2 VLAN translation (EFP to EFP), ingress port configuration:

  Switch (config)# interface gigabitethernet0/1
  Switch (config-if)# switchport trunk allowed vlan none
  Switch (config-if)# switchport mode trunk
  Switch (config-if)# service instance 10 Ethernet
  Switch (config-if-srv)# encapsulation dot1q 10
  Switch (config-if-srv)# rewrite ingress tag pop 1 symmetric
  Switch (config-if-srv)# bridge-domain 10

  Egress port configuration:

  Switch (config)# interface gigabitethernet0/2
  Switch (config-if)# switchport trunk allowed vlan none
  Switch (config-if)# switchport mode trunk
  Switch (config-if)# service instance 10 Ethernet
  Switch (config-if-srv)# encapsulation dot1q 20 second dot1q 30
  Switch (config-if-srv)# rewrite ingress tag pop 2 symmetric
  Switch (config-if-srv)# bridge-domain 10

- For 2-to-1 VLAN translation (EFP to EFP), ingress port configuration:

  Switch (config)# interface gigabitethernet0/1
  Switch (config-if)# switchport trunk allowed vlan none
  Switch (config-if)# switchport mode trunk
  Switch (config-if)# service instance 10 Ethernet
  Switch (config-if-srv)# encapsulation dot1q 10 second-dot1q 20
  Switch (config-if-srv)# rewrite ingress tag pop 2 symmetric
  Switch (config-if-srv)# bridge-domain 10

  Egress port configuration:

  Switch (config)# interface gigabitethernet0/2
  Switch (config-if)# switchport trunk allowed vlan none
  Switch (config-if)# switchport mode trunk
  Switch (config-if)# service instance 10 Ethernet
  Switch (config-if-srv)# encapsulation dot1q 30
  Switch (config-if-srv)# rewrite ingress tag pop 1 symmetric
Configuring Other Features on EFPs

Switch (config-if-srv)# bridge-domain 10

- For 2-to-2 VLAN translation (EFP to EFP), ingress port configuration:

  Switch (config)# interface gigabitethernet0/1
  Switch (config-if)# switchport trunk allowed vlan none
  Switch (config-if)# switchport mode trunk
  Switch (config-if)# service instance 10 Ethernet
  Switch (config-if-srv)# encapsulation dot1q 10 second-dot1q 20
  Switch (config-if-srv)# rewrite ingress tag pop 2 symmetric
  Switch (config-if-srv)# bridge-domain 10

Egress port configuration:

  Switch (config)# interface gigabitethernet0/2
  Switch (config-if)# switchport trunk allowed vlan none
  Switch (config-if)# switchport mode trunk
  Switch (config-if)# service instance 10 Ethernet
  Switch (config-if-srv)# encapsulation dot1q 30 second-dot1q 40
  Switch (config-if-srv)# rewrite ingress tag pop 2 symmetric
  Switch (config-if-srv)# bridge-domain 10

Layer 2 Protocol Tunneling

Customers at different sites connected across a service-provider network need to use various Layer 2 protocols to scale their topologies 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 network. 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 that are participating in VTP. Similarly, DTP, LACP, LLDP, PAgP, and UDLD can also run across the service-provider network.

When protocol tunneling is enabled, edge switches on the inbound side of the service-provider network encapsulate Layer 2 protocol packets with a special MAC address (0100.0CCD.CDD0) and send them across the service-provider network. Core switches in the network do not process these packets but forward them as normal (unknown multicast data) packets. Layer 2 protocol data units (PDUs) for the configured protocols cross the service-provider network 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 can 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 to all switches through the service provider that support VTP.

Customers use Layer 2 protocol tunneling to tunnel BPDUs through a service-provider network without interfering with internal provider network BPDUs.

Note

On ME 3800X and ME 3600X switches, Layer 2 protocol tunneling is supported on EFPs, but not on switchports. Layer 2 protocol tunneling is not supported on cross-connect EFPs.
In Figure 12-3, Customer X has four switches in the same VLAN, which 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 other Layer 2 protocols. 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 12-4.

Figure 12-3  Layer 2 Protocol Tunneling

Figure 12-4  Layer 2 Network Topology without Proper Convergence
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 12-5, 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.

Figure 12-5 Layer 2 Protocol Tunneling for EtherChannels

Use the `l2protocol tunnel protocol` service-instance configuration command to enable Layer 2 protocol tunneling on a service instance:

Valid protocols include CDP, DTP, LACP, LLDP, PAgP, STP, VTP, and UDLD. If a protocol is not specified for a service instance, the protocol frame is dropped at the interface.

This is an example of Layer 2 protocol tunneling configuration:

```
Switch (config)# interface gigabitethernet0/2
Switch (config)# switchport mode trunk
Switch (config)# switchport trunk allowed vlan none
Switch (config-if)# service instance 10 Ethernet
Switch (config-if-srv)# encapsulation untagged, dot1q 200 second-dot1q 300
Switch (config-if-srv)# l2protocol tunnel cdp stp vtp dtp pagp lacp
Switch (config-if-srv)# bridge-domain 10
```

Note

To enable tunneling of most Layer 2 protocol, you must configure `encapsulation untagged` because Layer 2 protocol PDUs are usually untagged.

**EFPs and Ethernet over Multiprotocol Layer Switching (EoMPLS)**

When you configure a pseudowire under a VLAN interface (for example, VLAN 33), the pseudowire becomes a virtual Layer 2 port in that VLAN (VLAN 33), or bridge domain. In this bridge domain, you can configure other types of Layer 2 ports, such as EFP ports and switchports. Switching functionalities, such as MAC address learning, flooding, and forwarding to learned MAC addresses, apply to all the Layer 2 ports, including the pseudowire.
When a pseudowire is present in the same bridge domain as an EFP, you cannot configure the EFP with the **rewrite ingress tag pop 2 symmetric** service instance configuration command. Other restrictions about switching between EFPs or between EFPs and switchports also still apply.

See the “EoMPLS and EVC” section on page 36-35 for more information and a configuration example.

### Bridge Domain Routing

The switch supports IP routing and multicast routing for bridge domains, including Layer 3 and Layer 2 VPNs, using the SVI model. There are the limitations:

- You must configure SVIs for bridge-domain routing.
- The bridge domain must be in the range of 1 to 4094 to match the supported VLAN range.
- You can use bridge domain routing with only native packets.
- MPLS is not supported.

This is an example of configuring bridge-domain routing with a single tag EFP:

```conf
Switch (config)# interface gigabitethernet0/2
Switch (config)# switchport mode trunk
Switch (config)# switchport trunk allowed vlan none
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation dot1q 10
Switch (config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch (config-if-srv)# bridge-domain 100

Switch (config)# interface vlan 100
Switch (config-if)# ip address 20.1.1.1 255.255.255.255
```

This is an example of configuring bridge-domain routing with two tags:

```conf
Switch (config)# interface gigabitethernet0/2
Switch (config)# switchport mode trunk
Switch (config)# switchport trunk allowed vlan none
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation dot1q 10 second-dot1q 20
Switch (config-if-srv)# rewrite ingress tag pop 2 symmetric
Switch (config-if-srv)# bridge-domain 100

Switch (config)# interface vlan 100
Switch (config-if)# ip address 20.1.1.1 255.255.255.255
```

### EFPs and Switchport MAC Addresses

Because forwarding can occur between EFPs and switchports, MAC address movement can occur on learned addresses. Addresses learned on EFPs will have the format of interface + EFP ID, for example gigabitethernet 0/1 + EFP 1. When an address moves between a non-secured EFP and a switchport, the behavior is similar to that of moving between switchports.

To see MAC address information for VLANs 1 to 4094, use the `show mac address-table vlan` privileged EXEC command. For VLANs 4096 to 8000, use the `show mac address-table bridge-domain` privileged EXEC command. All other `show mac address-table` commands also support bridge domains as well as VLANs.
When an EFP property changes (bridge domain, rewrite, encapsulation, split-horizon, secured or unsecured, or a state change), the old dynamic MAC addresses are flushed from their existing tables. This is to prevent old invalid entries from lingering.

**Note**
Static MAC addresses are not supported on EFPs, static MAC is only supported on switchports.

### EVC and Switchports

Bridging EFPs and switchports in the same switch is a typical configuration in the edge of the network where network-facing interfaces are switchports and user network interfaces are EVC ports where various VLAN rewrites take place. The user-facing interfaces have EVC configuration because the incoming VLANs are only significant on the ingress interface (customer VLANs), which requires VLAN tagging modification. All the network-facing interfaces have VLAN tags, which are globally significant in the provider network.

In order for EFPs and switchports to bridge frames to each other, they must belong to the same bridge domain. For switchports, the bridge domain is set to the incoming VLAN tags. The ingress rewritten VLAN tag at the customer interface would match the bridge domain ID, which represents an S-VLAN for the service provider.

**Network port configurations:**
```
Switch (config)# interface gigabitethernet0/10 - gigabitethernet0/11
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan 20-30
```

**Customer port configurations:**
```
Switch (config)# interface gigabitethernet0/1
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan none
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation dot1q 2000
Switch (config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch (config-if-srv)# bridge-domain 20
Switch (config-if-srv)# exit
Switch (config-if)# service instance 2 Ethernet
Switch (config-if-srv)# encapsulation dot1q 2001
Switch (config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch (config-if-srv)# bridge-domain 30
```

**Network port configurations:**
```
Switch (config)# interface gigabitethernet0/2
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan none
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation dot1q 3000
Switch (config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch (config-if-srv)# bridge-domain 20
Switch (config-if-srv)# exit
Switch (config-if)# service instance 2 Ethernet
Switch (config-if-srv)# encapsulation dot1q 3001
Switch (config-if-srv)# rewrite ingress tag pop 1 symmetric
Switch (config-if-srv)# bridge-domain 30
```

EVCs and switchports can exist simultaneously on the same switch. When an EFP joins a bridge domain 1 through 4095, it is part of the same flood domain as VLANs 1 through 4095. If an EFP uses a bridge domain greater than or equal to 4096, it belongs to the EFP-only flood domain.
This example shows VLANs and EFPs sharing the same flooding domain.

```plaintext
Switch (config)# interface gigabitethernet0/1
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan 1000

Switch (config)# interface gigabitethernet0/2
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation dot1q 1000
Switch (config-if-srv)# bridge-domain 1000
```

When data packets are forwarded between EFPs and switchports, the EFP and switchport configurations are applied to the packet. This removes the ambiguity of the tagging behavior between them.

The following illustrations show tagging behavior between an EFP and a switchport. A switchport trunk has an implicit outer VLAN pop at ingress and an implicit outer VLAN push at egress. When rewrite is enabled, a VLAN tag is popped at ingress and a VLAN tag corresponding to the bridge domain that bridged the packet is pushed at egress on the switchport trunk without any explicit configuration. When a VLAN tag is pushed on a packet egressing at the switchport, the VLAN ID corresponds to the bridge-domain ID over which the packet is bridged.

Figure 12-6 to Figure 12-8 show traffic between a switchport and an EFP when rewrite symmetric is enabled on the EFP.

**Figure 12-6  Single-tagged Traffic Between a Switchport and an EFP with Rewrite**

In this example, for traffic entering the switchport trunk port, the VLAN tag is popped on ingress at the switchport trunk port and the untagged packet is bridged over bridge domain 10. On egress, the rewrite operation results in a VLAN tag (encapsulation dot1q 10) to be pushed (added), and the packet egresses on the EFP with a single tag (VLAN 10).

For traffic entering the EFP, a VLAN tag is popped at the EFP with a rewrite and the untagged packet is bridged over bridge domain 10. At egress on the switchport trunk port, the VLAN tag corresponding to the bridge domain (VLAN 10) is pushed, and the packet egresses on the switchport with a single tag (VLAN 10).

**Figure 12-7  Double-tagged Traffic Between a Switchport and an EFP with Rewrite**
At ingress on the switchport, the outer most VLAN tag (VLAN 10) is popped at the switchport and the packet is bridged over bridge-domain 10 with a single tag (VLAN 20). On egress at the EFP with a rewrite, a VLAN tag equal to the encapsulation dot1q VLAN ID (10) is pushed, and the double-tagged packet (tagged with VLAN 10 and VLAN 20) goes out on the EFP.

For packets ingressing at the EFP, the outer most VLAN tag is popped at the EFP and the single-tagged packet (VLAN 10) is bridged over bridge-domain 10. On egress at the switchport, a VLAN tag equal to the bridge domain (VLAN 10) is pushed, and the double-tagged packet (VLAN 10 and 20) goes out the switchport.

**Figure 12-8 Untagged Traffic Between a Switchport (with Native or Access VLAN) and an EFP with Rewrite**

At ingress on the switchport, an untagged packet is bridged over bridge-domain 10. On egress at the EFP after a rewrite, a VLAN tag equal to the encapsulation dot1q VLAN (10) is pushed, and a single-tagged packet (VLAN 10) is sent out on the EFP.

For packets ingressing the EFP with a rewrite, a VLAN tag (VLAN 10) is popped at the EFP, and the untagged packet is bridged over bridge-domain 10. At egress on the switchport, the native VLAN or access VLAN matches the bridge-domain, and the packet is sent out as untagged.

**Figure 12-9 to Figure 12-12 show traffic between a switchport and an EFP with no rewrite.**

**Figure 12-9 Single-tagged Traffic Between a Switchport and an EFP with no Rewrite**

On ingress at the switchport, a VLAN tag is popped at the switchport trunk, and an untagged packet is bridged over bridge-domain 10. On egress at the EFP with no rewrite, there is an encapsulation mismatch because the bridged packet is untagged, and the encapsulation is 802.1q VLAN 10. Therefore, the packet is dropped.
Figure 12-10 Single-tagged and Double-tagged Traffic Between a Switchport and an EFP with no Rewrite

On ingress at the switchport, the outer most VLAN tag (VLAN 10) is popped at the switchport trunk and single-taged packet (VLAN 20) is bridged over bridge-domain 10. On egress at the EFP with no rewrite, the bridged packet tag (VLAN 20) matches the encapsulation, and a single-tagged packet (VLAN 20) is sent out on the EFP.

On ingress at the EFP with no rewrite, a single-tagged packet (VLAN 20) is bridged over bridge-domain 10. On egress at the switchport, a VLAN tag corresponding to the bridge-domain (VLAN 10) is pushed, and a double-tagged packet (VLAN 10 and VLAN 20) is sent out on the switchport.

Figure 12-11 Untagged Traffic From a Switchport (with Native or Access VLAN) to an EFP with No Rewrite

After ingress at the switchport, the untagged packet is bridged over bridge-domain 10. On egress at the EFP with no rewrite, there is an encapsulation mismatch because the bridged packet is untagged and the encapsulation is dot1q 10. Therefore, the packet is dropped.

The same scenario applies when the switchport trunk is configured with the access VLAN ID or native VLAN ID.

Figure 12-12 Single-tagged Traffic From an EFP with No Rewrite to a Switchport (with Native or Access VLAN)

After ingress at the EFP with no rewrite, the single tagged packet (VLAN 10) is bridged over bridge-domain 10. On egress at the switchport, the native VLAN matches the bridge-domain and a single-tagged (VLAN 10) packet is sent out the switchport.

The same scenario applies when the switchport trunk is configured with the access VLAN ID or native VLAN ID.
Note

Receiving a VLAN-tagged packet where the VLAN is equal to the switchport trunk native VLAN or the access VLAN is unexpected tagging behavior in switchport-only interactions. However, you can expect to receive tagged packets equal to the native VLAN or access VLAN when the switchport interacts with EFPs.

**EFPs and MSTP**

EFP bridge domains are supported by the Multiple Spanning Tree Protocol (MSTP). These restrictions apply when running STP with bridge domains.

- All incoming VLANs (outer-most or single) mapped to a bridge domain must belong to the same MST instance or loops could occur.
- For all EFPs that are mapped to the same MST instance, you must configure backup EFPs on every redundant path to prevent loss of connectivity due to STP blocking a port.
- When STP mode is PVST+ or PVRST, EFP information is not passed to the protocol. EVC only supports only MSTP.
- Changing STP mode from MST to PVST+ or PVRST for a multicast port is not allowed.

**L3 Unicast and Multicast Routing on a Bridge Domain with Multiple EFPs**

L3 unicast routing and L3 multicast routing are supported on bridge domains with multiple EFPs. This feature provides the following functionality:

- Broadcast domains are determined through bridge-domains rather than VLANs
- Multiple EFPs on a single bridge domain and physical interface with L3 multicast routing enabled is supported
- Each EFP has its own match criteria and its own ingress and egress rewrite operations
Figure 12-13 shows an access-facing port with multiple EFPs configured to the route or bridge.

Figure 12-13  Multiple EFPs

Restrictions
IRB is required for L3 termination at the SVI with redundant L2 links.
For core-based deployments, MPLS is a preferred transport for any traffic type.
Configuring L3 Multicast Routing on a Bridge Domain

No new CLI support is required to configure this feature.

The following example shows how to configure L3 multicast routing on a bridge domain using existing IOS commands. You can configure a maximum of 26 EFPs on the bridge domain.

    ip routing
    ip multicast-routing
    !
    interface vlan 100
    ip address 1.1.1.1 255.255.255.0
    ip pim sparse-mode
    igmp version v3
    !
    interface GigabitEthernet0/1
    switchport trunk allowed vlan none
    switchport mode trunk
    service instance 1 ethernet
    encapsulation dot1q 33
    rewrite ingress tag pop 1 symmetric
    bridge-domain 100
    !
    service instance 2 ethernet
    encapsulation dot1q 55
    rewrite ingress tag pop 1 symmetric
    bridge-domain 100
    
    service instance 3 ethernet
    encapsulation dot1q 66
    rewrite ingress tag pop 1 symmetric
    bridge-domain 100

Cross-Connect on EFP Interfaces

Cross-connect provides the ability to match the encapsulation of received packets on the ingress side of an EFP interface and send them out with the same encapsulation through the egress side of the EFP interface. Cross-connect bridge-domain entries are provided, and encapsulation matching is achieved by matching bridge-domain entries for the EFPs on which cross-connect is configured.

The following types of encapsulation tags are supported:

- untagged
- rewrite tags with pop1

Restrictions

- A bridge-domain cannot be configured on an EFP if cross-connect is already configured.
- Cross-connect works only when the MPLS license is enabled.
- Priority-tagged encapsulation is not supported.
#### Configuring Cross-Connect on an EFP Interface

Beginning in privileged EXEC mode, follow these steps to configure cross-Connect on an EFP Interface.

**Summary Steps**

1. `configure terminal`
2. `interface interface-id`
3. `service instance number ethernet [name]`
4. `encapsulation dot1q vlan_id cos cos_value second-dot1q vlan-id cos cos_value`
5. `xconnect peer-router-id vcid pw-class pw-class name`
6. `end`

**Detailed Steps**

<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>interface interface-id</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>service instance number ethernet [name]</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>encapsulation dot1q vlan_id cos cos_value second-dot1q vlan-id cos cos_value</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>xconnect peer-router-id vcid pw-class pw-class name</code></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>end</code></td>
</tr>
</tbody>
</table>

This is an example configuration of cross-connect on an EFP interface:

```
interface gigabitethernet 0/3
   service instance 30 ethernet
   encap dot1q x second dot1q y
   xconnect <10.10.10.10> 123 encapsulation mpls
```
### Monitoring EVC

#### Table 12-3 Supported show Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ethernet service evc [id evc-id] [interface interface-id] [detail]</td>
<td>Displays information about all EVCs, or a specific EVC when you enter an EVC ID, or all EVCs on an interface when you enter an interface ID. The <code>detail</code> option provides additional information about the EVC.</td>
</tr>
<tr>
<td>show ethernet service instance [id instance-id interface interface-id] [interface interface-id] [detail]</td>
<td>Displays information about one or more service instance (EFPs). If you specify an EFP ID and interface, only data pertaining to that particular EFP is displayed. If you specify only an interface ID, data is displayed for all EFPs on the interface.</td>
</tr>
<tr>
<td>show bridge-domain [n]</td>
<td>When you enter <code>n</code>, this command displays all the members of the specified bridge-domain, if a bridge-domain with the specified number exists. If you do not enter <code>n</code>, the command displays all the members of all bridge-domains in the system.</td>
</tr>
<tr>
<td>show bridge-domain n split-horizon [group {group_id</td>
<td>all}]</td>
</tr>
<tr>
<td>show ethernet service instance detail</td>
<td>This command displays detailed service instance information, including Layer 2 protocol information. This is an example of the output:</td>
</tr>
<tr>
<td></td>
<td><strong>Switch# show ethernet service instance detail</strong></td>
</tr>
<tr>
<td></td>
<td>Service Instance ID: 1</td>
</tr>
<tr>
<td></td>
<td>Associated Interface: Ethernet0/0</td>
</tr>
<tr>
<td></td>
<td>Associated EVC: L2protocol tunnel pagp</td>
</tr>
<tr>
<td></td>
<td>CE-Vlans:</td>
</tr>
<tr>
<td></td>
<td>State: Up</td>
</tr>
<tr>
<td></td>
<td>EFP Statistics:</td>
</tr>
<tr>
<td></td>
<td>Pkts In  Bytes In  Pkts Out  Bytes Out</td>
</tr>
<tr>
<td></td>
<td>0        0        0        0</td>
</tr>
<tr>
<td>show mac address-table</td>
<td>This command displays dynamically learned or statically configured MAC security addresses.</td>
</tr>
<tr>
<td>show mac address-table bridge-domain bridge-domain id</td>
<td>This command displays MAC address table information for the specified bridge domain.</td>
</tr>
<tr>
<td>show mac address-table count bridge-domain bridge-domain id</td>
<td>This command displays the number of addresses present for the specified bridge domain.</td>
</tr>
<tr>
<td>show mac address-table learning bridge-domain bridge-domain id</td>
<td>This command displays the learning status for the specified bridge domain.</td>
</tr>
</tbody>
</table>

This is an example of output from the `show ethernet service instance detail` command:

```
Switch# show ethernet service instance id 1 interface gigabitEthernet 0/1 detail
Service Instance ID: 1
Associated Interface: GigabitEthernet0/13
Associated EVC: EVC_P2P_10
```
L2protocol drop
CE-Vlans:
Encapsulation: dot1q 10 vlan protocol type 0x8100
Interface Dot1q Tunnel Ethertype: 0x8100
State: Up
EFP Statistics:
  Pkts In  Bytes In  Pkts Out  Bytes Out
  214  15408  97150  6994800
EFP Microblocks:
****************
Microblock type: Bridge-domain
Bridge-domain: 10

This is an example of output from the show ethernet service instance statistics command:
Switch# show ethernet service instance id 1 interface gigabitEthernet 0/13 stats
Service Instance 1, Interface GigabitEthernet0/13
Pkts In  Bytes In  Pkts Out  Bytes Out
  214  15408  97150  6994800

This is an example of output from the show mac-address table count command:
Switch# show mac address-table count bridge-domain 10
Mac Entries for BD 10:
------------------------
Dynamic Address Count : 20
Static  Address Count  : 0
Total Mac Addresses    : 20
CHAPTER 13

Configuring Command Macros

This chapter describes how to configure and apply command macros on the Cisco ME 3800X and ME 3600X switch.

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

- Understanding Command Macros, page 13-1
- Configuring Command Macros, page 13-1
- Displaying Command Macros, page 13-5

Understanding Command Macros

Command macros provide a convenient way to save and share common configurations. You can use command 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 command macro is a set of command-line interface (CLI) commands that you define. Command macros do not contain new CLI commands; they are simply a group of existing CLI commands.

When you apply a command 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.

Configuring Command Macros

You can create a new command 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, to a switch interface, or to a range of interfaces.

- Default Command Macro Configuration, page 13-2
- Command Macro Configuration Guidelines, page 13-2
- Creating Command Macros, page 13-3
- Applying Command Macros, page 13-4
- Displaying Command Macros, page 13-5
Default Command Macro Configuration

There are no command macros enabled.

Command 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.

- 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.

- When you apply a macro to a user network interface (UNI) or enhanced network interface (ENI), you must first enable the port. UNIs and ENIs are disabled by default.
Creating Command Macros

Beginning in privileged EXEC mode, follow these steps to create a command macro:

<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>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>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<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 Command Macros

Beginning in privileged EXEC mode, follow these steps to apply a command macro:

<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 macro global { apply</td>
<td>trace } macro-name [parameter {value}] [parameter {value}]</td>
</tr>
<tr>
<td>Step 3 macro global description text</td>
<td>(Optional) Enter a description about the macro that is applied to the switch.</td>
</tr>
<tr>
<td>Step 4 interface interface-id</td>
<td>(Optional) Enter interface configuration mode, and specify the interface on which to apply the macro.</td>
</tr>
<tr>
<td>Step 5 no shutdown</td>
<td>Enable the port, if necessary. By default, UNIs and enhanced network interfaces (ENIs) are disabled, and network node interfaces (NNIs) are enabled.</td>
</tr>
<tr>
<td>Step 6 default interface interface-id</td>
<td>(Optional) Clear all configuration from the specified interface.</td>
</tr>
<tr>
<td>Step 7 macro { apply</td>
<td>trace } macro-name [parameter {value}] [parameter {value}]</td>
</tr>
<tr>
<td>Step 8 macro description text</td>
<td>(Optional) Enter a description about the macro that is applied to the interface.</td>
</tr>
<tr>
<td>Step 9 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 10 show parser macro description [interface interface-id]</td>
<td>Verify that the macro is applied to the interface.</td>
</tr>
<tr>
<td>Step 11 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
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 gigabitethernet0/2
Switch(config-if)# macro apply desktop-config
Switch(config-if)# end
Switch# show parser macro description
Interface    Macro Description
--------------------------------------------------------------
Gi0/2  desktop-config
```

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
```

### Displaying Command Macros

To display the command macros, use one or more of the privileged EXEC commands in Table 13-1.

<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 macroname</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 STP

This chapter describes how to configure the Spanning Tree Protocol (STP) on port-based VLANs on the Cisco ME 3800X and ME 3600X switch. The switch can use the per-VLAN spanning-tree plus (PVST+) protocol based on the IEEE 802.1D standard and Cisco proprietary extensions, or the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol based on the IEEE 802.1w standard. On the Cisco ME switch, STP is enabled by default on physical interfaces.

For information about the Multiple Spanning Tree Protocol (MSTP) and how to map multiple VLANs to the same spanning-tree instance, see Chapter 15, “Configuring MSTP.” For information about other spanning-tree features such as Port Fast, root guard, and so forth, see Chapter 16, “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.

- Understanding Spanning-Tree Features, page 14-1
- Configuring Spanning-Tree Features, page 14-10
- Displaying the Spanning-Tree Status, page 14-22

Understanding Spanning-Tree Features

- STP Overview, page 14-2
- Spanning-Tree Topology and BPDUs, page 14-2
- Bridge ID, Switch Priority, and Extended System ID, page 14-3
- Spanning-Tree Interface States, page 14-4
- How a Switch or Port Becomes the Root Switch or Root Port, page 14-7
- Spanning Tree and Redundant Connectivity, page 14-7
- Spanning-Tree Address Management, page 14-8
- Accelerated Aging to Retain Connectivity, page 14-8
- Spanning-Tree Modes and Protocols, page 14-9
- Supported Spanning-Tree Instances, page 14-9
- Spanning-Tree Interoperability and Backward Compatibility, page 14-10
- STP and IEEE 802.1Q Trunks, page 14-10
For configuration information, see the “Configuring Spanning-Tree Features” section on page 14-10.

For information about optional spanning-tree features, see Chapter 16, “Configuring Optional Spanning-Tree Features.”

**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 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*

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.
Understanding Spanning-Tree Features

• The port identifier (port priority and MAC address) associated with each Layer 2 STP-enabled 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, or on the Cisco ME switch, only through the STP-enabled ports. The BPDUss 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 14-1 on page 14-4.

• 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 an 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 IEEE 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 14-1, 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.

### Table 14-1 Switch Priority Value and Extended System ID

<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>

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 14-14, the “Configuring a Secondary Root Switch” section on page 14-15, and the “Configuring the Switch Priority of a VLAN” section on page 14-19.

### 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 STP port 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.

A port participating in spanning tree 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 14-1 shows how an interface moves through the states.

**Figure 14-1 Spanning-Tree Interface States**

When you power up the switch, spanning tree is enabled by default, and every port on the switch, as well as any other port in other switches in the VLAN or network that are participating in spanning tree, 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 spanning-tree 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, or to each switch STP port. 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 participating in spanning tree 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 decides 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 14-2, 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.

Figure 14-2 Spanning-Tree Topology

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 that are participating in spanning tree to another device or to two different devices, as shown in Figure 14-3. 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.
You can also create redundant links between switches by using EtherChannel groups. For more information, see Chapter 28, “Configuring EtherChannels.”

**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 0x0180C20000F. 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 (as the forward-delay parameter value in the `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 ports support 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 most 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. This is the default spanning-tree mode for the Cisco ME switch NNIs. Rapid PVST+ is compatible with PVST+. 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 15, “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.
Spanning-Tree Interoperability and Backward Compatibility

Table 14-2 lists the interoperability and compatibility among the supported spanning-tree modes in a network.

<table>
<thead>
<tr>
<th></th>
<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>
<td>Yes (reverts to PVST+)</td>
</tr>
<tr>
<td>MSTP</td>
<td>Yes (with restrictions)</td>
<td>Yes</td>
<td>Yes (reverts to PVST+)</td>
</tr>
<tr>
<td>Rapid PVST+</td>
<td>Yes (reverts to 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 802.1Q switch.

However, all PVST+ or rapid-PVST+ information is maintained by Cisco switches separated by a cloud of non-Cisco 802.1Q switches. The non-Cisco 802.1Q cloud separating the Cisco switches is treated as a single trunk link between the switches.

PVST+ is automatically enabled on IEEE 802.1Q trunks, and no user configuration is required. The external spanning-tree behavior on access ports is not affected by PVST+.

For more information on IEEE 802.1Q trunks, see Chapter 11, “Configuring VLANs.”

Configuring Spanning-Tree Features

- Default Spanning-Tree Configuration, page 14-11
- Spanning-Tree Configuration Guidelines, page 14-11
- Changing the Spanning-Tree Mode., page 14-12 (required)
- Disabling Spanning Tree, page 14-13 (optional)
- Configuring the Root Switch, page 14-14 (optional)
• Configuring a Secondary Root Switch, page 14-15 (optional)
• Configuring Port Priority, page 14-16 (optional)
• Configuring Path Cost, page 14-18 (optional)
• Configuring the Switch Priority of a VLAN, page 14-19 (optional)
• Configuring Spanning-Tree Timers, page 14-20 (optional)

Default Spanning-Tree Configuration

Table 14-3 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 ports in VLAN 1.</td>
</tr>
<tr>
<td>Spanning-tree mode</td>
<td>Rapid PVST+</td>
</tr>
<tr>
<td></td>
<td>Rapid PVST+ interoperates with PVST and PVST+.</td>
</tr>
<tr>
<td></td>
<td>MSTP is disabled.</td>
</tr>
<tr>
<td>Switch priority</td>
<td>32768.</td>
</tr>
<tr>
<td>Spanning-tree port priority (configurable on</td>
<td>128.</td>
</tr>
<tr>
<td>a per-interface basis)</td>
<td></td>
</tr>
<tr>
<td>Spanning-tree port cost (configurable on a</td>
<td>1000 Mbps: 4.</td>
</tr>
<tr>
<td>per-interface basis)</td>
<td>100 Mbps: 19.</td>
</tr>
<tr>
<td></td>
<td>10 Mbps: 100.</td>
</tr>
<tr>
<td>Spanning-tree VLAN port priority (configurable on a per-VLAN basis)</td>
<td>128.</td>
</tr>
<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 than there are spanning-tree instances, you can enable PVST+ or rapid PVST+ on STP ports in 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 15, “Configuring MSTP.”

If 128 instances of spanning tree are already in use, you can disable spanning tree on STP ports in 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.
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.

If you have already used all available spanning-tree instances on your switch, adding another VLAN 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 STP port (an NNI or ENI with STP enabled) to a VLAN. The spanning-tree instance is removed when the last port 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 14-10.

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.

### Changing the Spanning-Tree Mode.

The switch supports three spanning-tree modes: PVST+, rapid PVST+, or MSTP. By default, the switch runs the rapid PVST+ protocol on all NNIs and ENIs on which spanning tree is enabled.

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></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>`spanning-tree mode { pvst</td>
<td>mst</td>
</tr>
<tr>
<td></td>
<td>• Select <code>pvst</code> to enable PVST+.</td>
</tr>
<tr>
<td></td>
<td>• Select <code>mst</code> to enable MSTP (and RSTP). For more configuration steps,</td>
</tr>
<tr>
<td></td>
<td>see Chapter 15, “Configuring MSTP”</td>
</tr>
<tr>
<td></td>
<td>• Select <code>rapid-pvst</code> to enable rapid PVST+ (the default setting).</td>
</tr>
</tbody>
</table>
## Configuring STP

### Configuring Spanning-Tree Features

To return to the default setting, use the `no spanning-tree mode` global configuration command. To return the port to its default spanning-tree mode setting, use the `no spanning-tree link-type` interface configuration command.

### Disabling Spanning Tree

Spanning tree is enabled by default on all ports in VLAN 1 and in all newly created VLANs up to the spanning-tree limit specified in the “Supported Spanning-Tree Instances” section on page 14-9. 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><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>no spanning-tree vlan vlan-id</code> For <code>vlan-id</code>, the range is 1 to 4094.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

---

**Command** | **Purpose**
---|---
Step 3 | `interface interface-id` *(Recommended only for rapid-PVST+ mode)* Specify an STP port 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 26.

Step 4 | `spanning-tree link-type point-to-point` *(Recommended only for rapid-PVST+ mode)* Specify that the link type for this port is point-to-point.

If you connect this 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 changes the local port to the forwarding state.

Step 5 | `end` Return to privileged EXEC mode.

Step 6 | `clear spanning-tree detected-protocols` *(Recommended only for rapid-PVST+ mode)* If any port on the switch running spanning tree is connected to a port on a legacy IEEE 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.
Configuring Spanning-Tree Features

Chapter 14  Configuring STP

Step 4

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show spanning-tree vlan vlan-id</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 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 14-1 on page 14-4.)

**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.

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>spanning-tree vlan vlan-id root primary [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>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 a Secondary Root Switch**

When you configure a 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><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>spanning-tree vlan vlan-id root secondary [diameter net-diameter [hello-time seconds]]</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show spanning-tree detail</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 root** global configuration command.

### Configuring Port Priority

If a loop occurs, spanning tree uses the port priority when selecting a spanning-tree port to put into the forwarding state. You can assign higher priority values (lower numerical values) to ports that you want selected first and lower priority values (higher numerical values) to ones that you want selected last. If all spanning-tree ports have the same priority value, spanning tree puts the port 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 a spanning-tree port. 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>
</tbody>
</table>
| Step 2  | interface interface-id | Specify an interface to configure, and enter interface configuration mode.  
|         |                     | **Note** If the interface is a VLAN, only ports with spanning tree enabled in the VLAN will run spanning tree.  
|         |                     | If the interface is a port channel, all members of the port channel must have spanning tree enabled. |
| Step 3  | spanning-tree port-priority priority | Configure the port priority for the spanning-tree port.  
|         |                     | For priority, the range is 0 to 240, in increments of 16; the default is 128. Valid values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected. The lower the number, the higher the priority. |
| Step 4  | spanning-tree vlan vlan-id port-priority priority | Configure the port priority for a VLAN.  
|         |                     | • 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 priority, the range is 0 to 240, in increments of 16; the default is 128. Valid values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected. The lower the number, the higher the priority. |
| Step 5  | end | Return to privileged EXEC mode. |
| Step 6  | show spanning-tree interface interface-id | Verify your entries. |
|         | or | show spanning-tree vlan vlan-id |
| Step 7  | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

---

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 spanning-tree 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 11-14.
Configuring Path Cost

The spanning-tree path cost default value is derived from the media speed of an interface (port running spanning tree or port channel of multiple ports running spanning tree). 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 NNIs (or port channels) have the same cost 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 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</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 cost cost</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>spanning-tree vlan vlan-id cost cost</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></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>or</td>
<td>show spanning-tree vlan vlan-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 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 11-14.

## Configuring the Switch Priority of a VLAN

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 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><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 14-4  Spanning-Tree Timers

<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 STP port begins forwarding.</td>
</tr>
<tr>
<td>Maximum-age timer</td>
<td>Controls the amount of time the switch stores protocol information received on an STP port.</td>
</tr>
</tbody>
</table>

Configuring the Hello Time

You can configure the interval between the generation of configuration messages by the root switch by changing the hello time.

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 hello time.

Beginning in privileged EXEC mode, follow these steps to configure the hello time of a VLAN. This procedure is optional.

Step 1 configure terminal
Enter global configuration mode.

Step 2 spanning-tree vlan vlan-id hello-time seconds
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.

- 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 seconds, the range is 1 to 10; the default is 2.

Step 3 end
Return to privileged EXEC mode.

Step 4 show spanning-tree vlan vlan-id
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 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><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>spanning-tree vlan <em>vlan-id</em> forward-time <em>seconds</em></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 <em>vlan-id</em></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

**Command Purpose**

**Step 1**
- **configure terminal**: Enter global configuration mode.

**Step 2**
- **spanning-tree vlan *vlan-id* forward-time *seconds***: Configure the forward time of a VLAN. The forward delay is the number of seconds a spanning-tree port waits before changing from its spanning-tree learning and listening states to the forwarding state.
  - 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 *seconds*, the range is 4 to 30; the default is 15.

**Step 3**
- **end**: Return to privileged EXEC mode.

**Step 4**
- **show spanning-tree vlan *vlan-id***: 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 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><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>spanning-tree vlan <em>vlan-id</em> max-age <em>seconds</em>**</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 <em>vlan-id</em></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

**Command Purpose**

**Step 1**
- **configure terminal**: Enter global configuration mode.

**Step 2**
- **spanning-tree vlan *vlan-id* max-age *seconds***: 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.
  - 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 *seconds*, the range is 6 to 40; the default is 20.

**Step 3**
- **end**: Return to privileged EXEC mode.

**Step 4**
- **show spanning-tree vlan *vlan-id***: 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 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 14-5:

Table 14-5 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 only on active spanning-tree interfaces.</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 spanning-tree 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.
Configuring MSTP

This chapter describes how to configure the Cisco implementation of the IEEE 802.1s Multiple STP (MSTP) on the Cisco ME 3800X and ME 3600X switch. STP is enabled by default on switch ports.

The multiple spanning-tree (MST) implementation is a pre-standard implementation. It is based on the draft version of the IEEE standard.

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 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 14, “Configuring STP.” For information about other spanning-tree features such as Port Fast, root guard, and so forth, see Chapter 16, “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.

- Understanding MSTP, page 15-2
- Understanding RSTP, page 15-8
- Configuring MSTP Features, page 15-14
- Displaying the MST Configuration and Status, page 15-27
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.

- Multiple Spanning-Tree Regions, page 15-2
- IST, CIST, and CST, page 15-2
- Hop Count, page 15-5
- Boundary Ports, page 15-6
- IEEE 802.1s Implementation, page 15-6
- Interoperability with IEEE 802.1D STP, page 15-8

For configuration information, see the “Configuring MSTP Features” section on page 15-14.

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 15-1 on page 15-4.

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. 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 BPDU 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.
Understanding MSTP

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 IEEE 802.1w, IEEE 802.1s, and IEEE 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 15-3 and the “Operations Between MST Regions” section on page 15-3.

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 15-1 on page 15-5.

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 15-1 on page 15-4), 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 IEEE 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 15-1 shows a network with three MST regions and a legacy IEEE 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 15-1  MST Regions, IST Masters, and the CST Root

---

Figure 15-1 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 IEEE 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 15-1 compares the IEEE standard and the Cisco prestandard terminology.

Table 15-1 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 BPDU 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 where 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 the example in Figure 15-1, 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.
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 15-2* 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.

![Standard and Prestandard Switch Interoperation](image)

**Note**

We recommend that you minimize the interaction between standard and prestandard MST implementations.

**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 15-3 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 IEEE 802.1D STP

A switch running MSTP supports a built-in protocol migration mechanism that enables it to interoperate with legacy IEEE 802.1D switches. If this switch receives a legacy IEEE 802.1D configuration BPDU (a BPDU with the protocol version set to 0), it sends only IEEE 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 IEEE 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. 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 IEEE 802.1D spanning tree), which is critical for networks carrying delay-sensitive traffic such as voice and video.

- Port Roles and the Active Topology, page 15-9
- Rapid Convergence, page 15-9
- Synchronization of Port Roles, page 15-11
- Bridge Protocol Data Unit Format and Processing, page 15-12

For configuration information, see the “Configuring MSTP Features” section on page 15-14.
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 14-2. 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 15-2 provides a comparison of IEEE 802.1D and RSTP port states.

### Table 15-2 Port State Comparison

<table>
<thead>
<tr>
<th>Operational Status</th>
<th>STP Port State (IEEE 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.

**Note** On the Cisco ME switch, these ports are always NNIs or STP-enabled ENIs.

As shown in Figure 15-4, 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.
Figure 15-4 Proposal and Agreement Handshaking for Rapid Convergence

Switch A  Proposal  Switch B

Root  Agreement  Designated switch
F  F  F
RP  DP  RP

Root  Designated switch  Proposal  Switch C
F  F  F
RP  DP  RP

Root  Designated switch  Agreement  Switch C
F  F  F
RP  DP  RP

DP = designated port
RP = root port
F = forwarding

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 STP 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 15-5.
Understanding RSTP

Figure 15-5  Sequence of Events During Rapid Convergence

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 15-3 shows the RSTP flag fields.

<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>

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.

### Topology Changes

This section describes the differences between the RSTP and the IEEE 802.1D in handling spanning-tree topology changes.

- **Detection**—Unlike IEEE 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 IEEE 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 IEEE 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 IEEE 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 IEEE 802.1D switches, RSTP selectively sends IEEE 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 IEEE 802.1D BPDU after the port’s migration-delay timer has expired, it assumes that it is connected to an IEEE 802.1D switch and starts using only IEEE 802.1D BPDUs. However, if the RSTP switch is using IEEE 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 MSTAFeatures

- Default MSTP Configuration, page 15-14
- MSTP Configuration Guidelines, page 15-15
- Specifying the MST Region Configuration and Enabling MSTP, page 15-16 (required)
- Configuring the Root Switch, page 15-17 (optional)
- Configuring a Secondary Root Switch, page 15-18 (optional)
- Configuring Port Priority, page 15-19 (optional)
- Configuring Path Cost, page 15-21 (optional)
- Configuring the Switch Priority, page 15-22 (optional)
- MSTP and Ethernet Flow Points (EFPs), page 15-23 (optional)
- Configuring the Hello Time, page 15-23 (optional)
- Configuring the Forwarding-Delay Time, page 15-23 (optional)
- Configuring the Maximum-Aging Time, page 15-24 (optional)
- Configuring the Maximum-Hop Count, page 15-24 (optional)
- Specifying the Link Type to Ensure Rapid Transitions, page 15-25 (optional)
- Designating the Neighbor Type, page 15-26 (optional)
- Restarting the Protocol Migration Process, page 15-26 (optional)

### Default MSTP Configuration

Table 15-4 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>Rapid PVST+ (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>
</tbody>
</table>
Configuring MSTP Features

For information about the supported number of spanning-tree instances, see the “Supported Spanning-Tree Instances” section on page 14-9.

MSTP Configuration Guidelines

- 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 14-10. For information on the recommended trunk port configuration, see the “Interaction with EtherChannels” section on page 11-11.
- 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.
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 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. 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</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>spanning-tree mst configuration</td>
</tr>
<tr>
<td></td>
<td>Enter MST configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>instance instance-id vlan vlan-range</td>
</tr>
<tr>
<td></td>
<td>Map VLANs to an MST instance.</td>
</tr>
<tr>
<td></td>
<td>• For instance-id, the range is 0 to 4094.</td>
</tr>
<tr>
<td></td>
<td>• For vlan vlan-range, the range is 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>To specify a VLAN range, use a hyphen; for example, instance 1 vlan 1-63 maps VLANs 1 through 63 to MST instance 1.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Step 4</td>
<td>name name</td>
</tr>
<tr>
<td></td>
<td>Specify the configuration name. The name string has a maximum length of 32 characters and is case sensitive.</td>
</tr>
<tr>
<td>Step 5</td>
<td>revision version</td>
</tr>
<tr>
<td></td>
<td>Specify the configuration revision number. The range is 0 to 65535.</td>
</tr>
<tr>
<td>Step 6</td>
<td>show pending</td>
</tr>
<tr>
<td></td>
<td>Verify your configuration by displaying the pending configuration.</td>
</tr>
<tr>
<td>Step 7</td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td>Apply all changes, and return to global configuration mode.</td>
</tr>
<tr>
<td>Step 8</td>
<td>spanning-tree mode mst</td>
</tr>
<tr>
<td></td>
<td>Enable MSTP. RSTP is also enabled.</td>
</tr>
</tbody>
</table>

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 rapid PVST+ or both MSTP and 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. |
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 rapid 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
Instance Vlans Mapped
--------  ---------------------
0         1-9,21-4094
1         10-20
-----------------------------

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 14-1 on page 14-4.)

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.
Configuring MSTP Features

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><code>spanning-tree mst instance-id root primary</code> <code>[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><strong>Step 3</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>show spanning-tree mst instance-id</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>copy running-config startup-config</code></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 a 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>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 secondary [diameter net-diameter [hello-time seconds]]</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 Port Priority

If a loop occurs, the MSTP uses the port priority when selecting an STP port to put into the forwarding state. You can assign higher priority values (lower numerical values) to STP ports 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>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.</td>
</tr>
<tr>
<td></td>
<td>Valid interfaces include physical NNIs or ENIs with spanning tree enabled, VLANs, and NNI or ENI port channels. The VLAN ID range is 1 to 4094. The port-channel range is 1 to 48.</td>
</tr>
<tr>
<td></td>
<td>Note: If a physical interface is a UNI, before attempting to configure MST port priority, you must enter the port-type mni interface configuration command or configure the port as an ENI and enable spanning tree on the port. See “Changing the Spanning-Tree Mode.” section on page 14-12.</td>
</tr>
<tr>
<td></td>
<td>If the interface is a VLAN, only ports with spanning tree enabled in the VLAN will run spanning tree.</td>
</tr>
<tr>
<td></td>
<td>If the interface is a port channel, all members of the port channel must be NNIs or ENIs with spanning tree enabled.</td>
</tr>
<tr>
<td>Step 3: spanning-tree mst instance-id port-priority priority</td>
<td>Configure the port priority.</td>
</tr>
<tr>
<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>- For priority, the range is 0 to 240 in increments of 16. The default is 128. The lower the number, the higher the priority.</td>
</tr>
<tr>
<td></td>
<td>The priority values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected.</td>
</tr>
<tr>
<td>Step 4: end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5: show spanning-tree mst interface interface-id or show spanning-tree mst instance-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>

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 STP port. 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 STP ports 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 NNIs or ENIs with spanning tree enabled, VLANs, and NNI or ENI port channels. The VLAN ID range is 1 to 4094. The port-channel range is 1 to 48. Note If a physical interface is a UNI, before attempting to configure MST port priority, you must enter the port-type nni interface configuration command or configure the port as an ENI and enable spanning tree on the port. See “Changing the Spanning-Tree Mode.” section on page 14-12. If the interface is a VLAN, only ports with spanning tree enabled in the VLAN will run spanning tree. If the interface is a port channel, all members of the port channel must be NNIs or ENIs with spanning tree enabled.</td>
</tr>
<tr>
<td>Step 3 spanning-tree mst instance-id cost cost</td>
<td>Configure the cost. If a loop occurs, the MSTP uses the path cost when selecting an interface to place into the forwarding state. A lower path cost represents higher-speed transmission. 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. For cost, the range is 1 to 200000000; the default value is derived from the media speed of the interface.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show spanning-tree mst 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>
The show spanning-tree mst 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 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.

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 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 spanning-tree mst instance-id priority priority</td>
<td>Configure the switch priority.</td>
</tr>
<tr>
<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>• For priority, 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 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show spanning-tree mst instance-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 the switch to its default setting, use the no spanning-tree mst instance-id priority global configuration command.
MSTP and Ethernet Flow Points (EFPs)

For MSTP to peer with a neighbor on a port that has an Ethernet Virtual Connection (EVC) EFP service instance configured, you need to enter the `l2 protocol peer stp` service-instance configuration command on the service instance. See the “Configuring Ethernet Virtual Connections (EVCs)” chapter for more information on EFPs.

This example shows how to configure Layer 2 protocol peer on a service instance:

```
Switch (config)# interface gigabitethernet0/1
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan none
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation untagged
Switch (config-if-srv)# l2protocol peer stp
Switch (config-if-srv)# bridge-domain 10
Switch (config-if-srv)# end
```

Configuring the Hello Time

You can configure the interval between the generation of configuration messages by the root switch by changing the hello time.

---

**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 hello time.

---

Beginning in privileged EXEC mode, follow these steps to configure the hello time for all MST instances. 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 hello-time seconds</td>
<td>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 seconds, the range is 1 to 10; the default is 2.</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</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 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.
Configuring MSTP Features

Chapter 15 Configuring MSTP

Converting MSTP Features

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><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>spanning-tree mst max-age seconds</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</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 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><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>spanning-tree mst forward-time seconds</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</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 forward-time` global configuration command.
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 an STP port to another STP 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 15-9.

By default, the link type is controlled from the duplex mode of the interface: 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</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>spanning-tree mst max-hops <code>hop-count</code></td>
</tr>
<tr>
<td></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</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 mst</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 the port to its default setting, use the `no spanning-tree link-type` interface configuration command.
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>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 mst pre-standard</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show spanning-tree mst interface interface-id</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>
```

To return the port to its default setting, use the `no spanning-tree mst prestandard` 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 interface, 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 15-5:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show spanning-tree mst configuration</td>
<td>Displays the MST region configuration.</td>
</tr>
<tr>
<td>show spanning-tree mst configuration digest</td>
<td>Displays the MD5 digest included in the current MSTCI.</td>
</tr>
<tr>
<td>show spanning-tree mst instance-id</td>
<td>Displays MST information for the specified instance.</td>
</tr>
<tr>
<td>show spanning-tree mst interface interface-id</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.
Configuring Optional Spanning-Tree Features

This chapter describes how to configure optional spanning-tree features on the Cisco ME 3800X and ME 3600X switch. You can configure all of these features when your switch is running 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. STP is enabled by default on switch ports.

For information on configuring the PVST+ and rapid PVST+, see Chapter 14, “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 15, “Configuring MSTP.”

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

- Understanding Optional Spanning-Tree Features, page 16-1
- Configuring Optional Spanning-Tree Features, page 16-5
- Displaying the Spanning-Tree Status, page 16-10

Understanding Optional Spanning-Tree Features

- Understanding Port Fast, page 16-2
- Understanding BPDU Guard, page 16-2
- Understanding BPDU Filtering, page 16-3
- Understanding EtherChannel Guard, page 16-3
- Understanding Root Guard, page 16-3
- Understanding Loop Guard, page 16-4
Understanding Port Fast

Port Fast immediately brings an STP port 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 STP ports connected to a single workstation or server, as shown in Figure 16-1, to allow those devices to immediately connect to the network, rather than waiting for the spanning tree to converge.

STP ports connected to a single workstation or server should not receive bridge protocol data units (BPDUs). An STP port 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 STP ports 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.

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 STP ports by using the `spanning-tree portfast bpduguard default` global configuration command. Spanning tree shuts down STP ports that are in a Port Fast-operational state if any BPDU is received on those ports. In a valid configuration, Port Fast-enabled STP ports do not receive BPDUs. Receiving a BPDU on a Port Fast-enabled port 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 STP port by using the `spanning-tree bpduguard enable` interface configuration command without also enabling the Port Fast feature. When the STP port 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 STP ports 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 ports do not receive BPDUs. If a BPDU is received on a Port Fast-enabled STP port, the interface loses its Port Fast-operational status, and BPDU filtering is disabled.

At the interface level, you can enable BPDU filtering on any STP port 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 STP port 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 STP port.

**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 STP ports 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 28-9.

If the switch detects a misconfiguration on the other device, EtherChannel guard places the switch STP ports 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 16-2. 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.

---

**Figure 16-2 Root Guard in a Service-Provider Network**

---

**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.
Chapter 16        Configuring Optional Spanning-Tree Features

Configuring Optional Spanning-Tree Features

- Default Optional Spanning-Tree Configuration, page 16-5
- Optional Spanning-Tree Configuration Guidelines, page 16-5
- Enabling Port Fast, page 16-5 (optional)
- Enabling BPDU Guard, page 16-6 (optional)
- Enabling BPDU Filtering, page 16-7 (optional)
- Enabling EtherChannel Guard, page 16-8 (optional)
- Enabling Root Guard, page 16-9 (optional)
- Enabling Loop Guard, page 16-9 (optional)

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 STP port).</td>
</tr>
<tr>
<td>EtherChannel guard</td>
<td>Globally enabled.</td>
</tr>
<tr>
<td>Root guard</td>
<td>Disabled on all STP ports.</td>
</tr>
<tr>
<td>Loop guard</td>
<td>Disabled on all STP ports.</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.

Enabling Port Fast

An STP port with the Port Fast feature enabled is moved 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.

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><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>Specify an STP interface to configure, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>spanning-tree portfast [trunk]</td>
</tr>
<tr>
<td></td>
<td>Enable Port Fast on an access port connected to a single workstation or server. By specifying the trunk keyword, you can enable Port Fast on a trunk port.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> To enable Port Fast on trunk ports, you must use the spanning-tree portfast trunk interface configuration command. The spanning-tree portfast command does not work on trunk ports.</td>
</tr>
<tr>
<td></td>
<td><strong>Caution</strong> 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><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 spanning-tree interface interface-id portfast</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>

**Note** You can use the spanning-tree portfast default global configuration command to globally enable the Port Fast feature on all nontrunking STP 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.
Configure Port Fast only on STP ports 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 STP port 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.

### Enabling BPDU Filtering

When you globally enable BPDU filtering on Port Fast-enabled STP ports, 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 BPDU is received on a Port Fast-enabled STP port, the interface loses its Port Fast-operational status, and BPDU filtering is disabled.

Configure Port Fast only on STP ports 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 STP port without also enabling the Port Fast feature. This command prevents the STP port from sending or receiving BPDUs.

Caution

Enabling BPDU filtering on an STP port 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> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> spanning-tree portfast bpdufilter default</td>
<td>Globally enable BPDU filtering. (By default, BPDU filtering is disabled.) Note: Globally enabling BPDU filtering enables it only on STP ports; the command has no effect on UNIs or ENIs on which STP is not enabled.</td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Specify the interface connected to an end station, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> spanning-tree portfast</td>
<td>Enable the Port Fast feature.</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 running-config</td>
<td>Verify your entries.</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>

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 on an STP port.

### 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><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> spanning-tree etherchannel guard misconfig</td>
<td>Enable EtherChannel guard.</td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Chapter 16  Configuring Optional Spanning-Tree Features

Configuring Optional Spanning-Tree Features

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 STP 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 STP port applies to all the VLANs to which the port belongs.

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 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.</td>
</tr>
<tr>
<td>Step 3 spanning-tree guard root</td>
<td>Enable root guard on the STP port.</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 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 STP ports 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>show spanning-tree active or show spanning-tree mst</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 3</td>
<td>spanning-tree loopguard default</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 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 on an NNI.

### Displaying the Spanning-Tree Status

Table 16-2 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 interface-id</td>
<td>Displays spanning-tree information for the specified interface.</td>
</tr>
<tr>
<td>show spanning-tree mst interface interface-id</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 Cisco ME 3800X and ME 3600X switch. REP is a Cisco proprietary protocol that provides an alternative to Spanning Tree Protocol (STP) to control network loops, to respond to link failures, and to 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.

Note
REP is not supported on ports configured with service instances.

This chapter includes these sections:
- Understanding REP, page 17-1
- Configuring REP, page 17-6
- Monitoring REP, page 17-14

Understanding REP

A REP segment is a chain of ports connected to each other and configured with a segment ID. Each segment consists of standard (nonedge) segment ports and two user-configured edge ports. A switch can have only two ports belonging 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 17-1 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 network failure, as shown in the diagram on the right, the blocked port returns to the forwarding state to minimize network disruption.
Understanding REP

Figure 17-1 REP Open Segments

The segment shown in Figure 17-1 is an open segment; there is no connectivity between the two edge ports. The REP segment cannot cause a bridging loop, and you can safely 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 host cannot access its usual gateway because of a failure, REP unblocks all ports to ensure that connectivity is available through the other gateway.

The segment shown in Figure 17-2, 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 17-2 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 17-3. 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.

When an edge port is configured with the **no-neighbor** and **rep stcn stp** commands MST will be enabled on the edge ports in order to send out STP TCNs.

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 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. After 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. The primary edge port 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:

- Enter 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.
- Enter 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 identify the secondary edge port (offset number -1) and its downstream neighbors.

**Note**

You configure offset numbers on the primary edge port by identifying the 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 17-4 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 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 17-4  Neighbor Offset Numbers in a Segment

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.

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 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 preemption 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.
Chapter 17 Configuring Resilient Ethernet Protocol

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.

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 to 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 changes 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 open 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, one as 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 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 messages.

- Default REP Configuration, page 17-7
- REP Configuration Guidelines, page 17-7
- Configuring the REP Administrative VLAN, page 17-8
- Configuring REP Interfaces, page 17-9
- Configuring SNMP Traps for REP, page 17-13
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

- 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 goes into 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. REP ports cannot be access ports.
- REP is not supported on ports configured with service instances.
- Be careful when configuring REP through a Telnet connection. Because REP blocks all VLANs until another REP interface sends a message to unblock the VLAN, you might lose connectivity to the switch if you enable REP in a Telnet session that accesses the switch through the REP 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 and remain 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 lsl-age-timer value` interface configuration command to set the time from 920 ms to 10000 ms. The LSL hello timer is then set to the age-timer value divided by three. In normal operation, three LSL hellos are sent before the age timer on the peer switch expires and searches for hello messages.
  - If the REP neighbor device is running software earlier than Cisco IOS Release 12.2(52)SE, the LSL age-timer range is from 3000 to 10000 ms in 500-ms increments. In that case, you must use the shorter time range because the device will not accept values out of the previous 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 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.

• When an edge port is configured with the `no-neighbor` and `rep stcn stp` commands MST will be enabled on the edge ports in order to send out STP TCNs.

### 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.

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>Step 1  <code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2  <code>rep admin vlan vlan-id</code></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 <code>no rep admin vlan</code> global configuration command.</td>
</tr>
<tr>
<td>Step 3  <code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4  <code>show interface [interface-id] rep detail</code></td>
<td>Verify the configuration on one of the REP interfaces.</td>
</tr>
<tr>
<td>Step 5  <code>copy running-config startup config</code></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 to 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 gigabitethernet0/1 rep detail
GigabitEthernet0/1 REP enabled
Segment-id: 2 (Edge)
PortID: 00010019E714680
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
EPA-ELECTION TLV rx: 118, tx: 118
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 4214, tx: 4190

Configuring REP Interfaces

For REP operation, you need to enable it on each segment interface and to 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.

Note: You cannot configure REP on interfaces that are configured with EVC service instances.

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</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, and enter interface configuration mode. The</td>
</tr>
<tr>
<td></td>
<td>interface can be a physical Layer 2 interface or a port channel</td>
</tr>
<tr>
<td></td>
<td>(logical interface). The port-channel range is 1 to 26.</td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport mode trunk</td>
</tr>
<tr>
<td></td>
<td>Configure the interface as a Layer 2 trunk port.</td>
</tr>
</tbody>
</table>
**Step 4**

```markdown
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. Enter `edge` without the `primary` keyword to configure the port as the secondary edge port. Each segment has only two edge ports.
- (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**

If `rep stcn stp` is configured MST will be enabled on this port.

- (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.

**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 set the port as 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**

```markdown
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.

**Note**

If the `no-neighbor` keyword is specified MST will be enabled on the port.
### Step 6
**Command**
```
rep block port {id port-id | neighbor_offset | preferred} vlan {vlan-list | all}
```

**Purpose**
(Optional) Configure VLAN load balancing on the primary edge port, identify the REP alternate port, 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 identifying 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 17-4 on page 17-5 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
**Command**
```
rep preempt delay seconds
```

**Purpose**
(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
**Command**
```
rep lsl-age-timer value
```

**Purpose**
(Optional) Configure a time (in milliseconds) for which the REP interface remains up without receiving a hello from a neighbor. The range is from 920 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(SE) or later, it will only accept 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
**Command**
```
end
```

**Purpose**
Return to privileged EXEC mode.

### Step 10
**Command**
```
show interface [interface-id] rep [detail]
```

**Purpose**
Verify the REP interface configuration.

### Step 11
**Command**
```
copy running-config startup config
```

**Purpose**
(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 gigabitethernet0/1
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 lsl-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 gigabitethernet0/1
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 lsl-age-timer 6000

This example shows how to configure the VLAN blocking configuration shown in Figure 17-5. 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 0/1).

Switch# configure terminal
Switch (conf)# interface gigabitethernet0/1
Switch (conf-if)# rep segment 1 edge primary
Switch (conf-if)# rep block port 4 vlan 100-200
Switch (conf-if)# end

**Figure 17-5  Example of VLAN Blocking**
Chapter 17 Configuring Resilient Ethernet Protocol

Configuring REP

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 to complete all other segment configuration 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.

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>rep preempt segment segment-id</td>
</tr>
<tr>
<td></td>
<td>show rep topology</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 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 snmp mib rep trap-rate value</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 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show running-config</td>
<td>Verify the REP trap 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 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

Table 17-1  REP Monitoring Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interface [interface-id] rep [detail]</code></td>
<td>Displays REP configuration and status for a specified interface or for all interfaces.</td>
</tr>
<tr>
<td><code>show rep topology [segment segment_id]</code></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>

[Segmentation]
CHAPTER 18

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 Cisco ME 3800X and ME 3600X switch that are used to 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

Flex Links and MAC address-table move update are not supported on ports configured with service instances.

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

- Understanding Flex Links and the MAC Address-Table Move Update, page 18-1
- Configuring Flex Links and MAC Address-Table Move Update, page 18-7
- Monitoring Flex Links and the MAC Address-Table Move Update, page 18-13

Understanding Flex Links and the MAC Address-Table Move Update

- Flex Links, page 18-1
- VLAN Flex Link Load Balancing and Support, page 18-2
- Flex Link Multicast Fast Convergence, page 18-3
- MAC Address-Table Move Update, page 18-6

Flex Links

Flex Links are a pair of a Layer 2 interfaces (switchports 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), allowing users to turn off STP and still provide 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, it is not necessary to configure Flex Links because STP already provides link-level redundancy or backup.
STP is enabled by default on the switch ports.

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. You cannot configure Flex Links on ports configured with an Ethernet virtual connection (EVC) service instance. 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 18-1, 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 18-1, for example, you can configure the Flex Link pair with preemption mode so that after port 1 comes back up in the scenario, if 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, Layer 3 ports, or ports configured with service instances.

**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 mrouter Port, page 18-3
- Generating IGMP Reports, page 18-3
- Leaking IGMP Reports, page 18-4

Learning the Other Flex Link Port as the mrouter 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

This configuration example shows learning the other Flex Link port as the mrouter port when Flex Link is configured on GigabitEthernet 0/11 and GigabitEthernet 0/12. The example shows the output for the `show interfaces switchport backup` command:

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet0/11
Switch(config-if)# switchport backup interface Gi0/12
Switch(config-if)# exit
Switch(config-if)# interface GigabitEthernet0/12
Switch(config-if)# end
Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface Backup Interface State
GigabitEthernet0/11 GigabitEthernet0/12 Active Up/Backup Standby
Preemption Mode : off
Multicast Fast Convergence : Off
Bandwidth : 100000 Kbit (Gi0/11), 100000 Kbit (Gi0/12)
Mac Address Move Update Vlan : auto
```

This output shows a querier for VLANs 1 and 401, with their queries reaching the switch through GigabitEthernet 0/11:

```
Switch# show ip igmp snooping querier
Vlan  IP Address  IGMP Version  Port
-----------------------------------------------
    1     1.1.1.1     v2     Gi0/11
   401   41.41.41.1     v2     Gi0/11
```
This 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), Gi0/12(dynamic)
401   Gi1/0/11(dynamic), Gi0/12(dynamic)
```

Similarly, both Flex Link ports are part of learned groups. In this example, GigabitEthernet 0/10 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     Gi0/11, Gi0/12, Gi0/10
 1      228.1.5.2 igmp  v2     Gi0/11, Gi0/12, Gi0/10
```

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 GigabitEthernet 0/11, because the backup port GigabitEthernet 0/12 is blocked. When the active link, GigabitEthernet 0/11, goes down, the backup port, GigabitEthernet 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 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 gigabitEthernet0/11
Switch(config-if)# switchport backup interface gigabitEthernet0/12 multicast fast-convergence
Switch(config-if)# exit
Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:                      
Active Interface Backup Interface State
--------------------------------------------------
GigabitEthernet0/11 GigabitEthernet0/12 Active Up/Backup Standby
Preemption Mode : off
Multicast Fast Convergence : On
Bandwidth : 100000 Kbit (Gi0/11), 100000 Kbit (Gi0/12)
Mac Address Move Update Vlan : auto
```

This output shows a querier for VLAN 1 and 401 with their queries reaching the switch through GigabitEthernet 0/11:

```
Switch# show ip igmp snooping querier
Vlan  IP Address  IGMP Version Port
------- ---------- ----- -------
 1      1.1.1.1    v2      Gi0/11
 1      1.1.1.1    v2      Gi0/11
```

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    Gi0/11(dynamic), Gi0/12(dynamic)
401   Gi0/11(dynamic), Gi0/12(dynamic)
```
Chapter 18      Configuring Flex Links and the MAC Address-Table Move Update Feature

Understanding Flex Links and the MAC Address-Table Move Update

Similarly, both the Flex Link ports are a part of the learned groups. In this example, GigabitEthernet 0/10 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    G10/11, G10/12, G10/10
1   228.1.5.2 igmp v2    G11/0/11, G10/12, G10/10
```

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 port, and when a report is forwarded by the switch on GigabitEthernet 0/11, it is also leaked to the backup port GigabitEthernet 0/12. The upstream router learns the groups and starts forwarding multicast data, which is dropped at the ingress because GigabitEthernet 0/12 is blocked. When the active link, GigabitEthernet 0/11, goes down, the backup port, Gigabiteternet t0/12, 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 18-3, 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 18-3 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

- Default Configuration, page 18-7
- Configuration Guidelines, page 18-8
- Configuring Flex Links, page 18-8
- Configuring VLAN Load Balancing on Flex Links, page 18-10
- Configuring the MAC Address-Table Move Update Feature, page 18-11

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.
Chapter 18
Configuring Flex Links and the MAC Address-Table Move Update Feature

Configuration Guidelines

- 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.
- You cannot configure Flex Links on ports configured with an Ethernet virtual connection (EVC) service instance.
- 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 (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. If STP is configured on the switch, Flex Links do not participate in STP in all VLANs in which STP is configured. With STP not running, 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><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 backup interface interface-id</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
</tbody>
</table>
Chapter 18  Configuring Flex Links and the MAC Address-Table Move Update Feature

Configuring Flex Links and MAC Address-Table Move Update

This example shows how to configure an interface with a backup interface and to verify the configuration:

Switch# configure terminal
Switch(conf)# interface gigabitethernet0/1
Switch(conf-if)# switchport backup interface gigabitethernet0/2
Switch(conf-if)# end
Switch# show interface switchport backup
Switch Backup Interface Pairs:

<table>
<thead>
<tr>
<th>Active Interface</th>
<th>Backup Interface</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/1</td>
<td>GigabitEthernet0/2</td>
<td>Active Up/Backup Standby</td>
</tr>
<tr>
<td>GigabitEthernet0/3</td>
<td>GigabitEthernet0/4</td>
<td>Active Up/Backup Standby</td>
</tr>
<tr>
<td>Port-channel1</td>
<td>GigabitEthernet0/1</td>
<td>Active Up/Backup Standby</td>
</tr>
</tbody>
</table>

Beginning in privileged EXEC mode, follow these steps to configure a preemption scheme for a pair of Flex Links:

**Command** | **Purpose**
--- | ---
Step 1 | configure terminal
| Enter global configuration mode. |
Step 2 | interface interface-id
| 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 26. |
Step 3 | switchport backup interface interface-id
| 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. |
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 as: |
| - **forced**—the active interface always preempts the backup. |
| - **bandwidth**—the interface with the 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 time delay 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. |
This example shows how to configure the preemption mode as forced for a backup interface pair and to verify the configuration:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport backup interface gigabitethernet0/2 preemption mode forced
Switch(config-if)# switchport backup interface gigabitethernet0/2 preemption delay 50
Switch(config-if)# end

Switch# show interface switchport backup detail
Active Interface Backup Interface State
-----------------------------------------------
GigabitEthernet0/21 GigabitEthernet0/2 Active Up/Backup Standby
Interface Pair : Gi0/1, Gi0/2
Preemption Mode : forced
Preemption Delay : 50 seconds
Bandwidth : 100000 Kbit (Gi0/1), 100000 Kbit (Gi0/2)
Mac Address Move Update Vlan : auto
```

### 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><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><code>switchport backup interface interface-id prefer vlan vlan-range</code></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] switchport backup</code></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>copy running-config startup config</code></td>
</tr>
</tbody>
</table>

In the following example, VLANs 1 to 50, 60, and 100 to 120 are configured on the switch:

```
Switch(config)# interface gigabitEthernet 0/6
Switch(config-if)# switchport backup interface gigabitEthernet 0/8 prefer vlan 60,100-120
```

When both interfaces are up, gigabitethernet port 0/8 forwards traffic for VLANs 60 and 100 to 120 and gigabitethernet port 0/6 forwards traffic for VLANs 1 to 50.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
Active Interface         Backup Interface         State
-----------------------------------------------
GigabitEthernet0/6      GigabitEthernet0/8    Active Up/Backup Standby
```

```
```
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 gigabitethernet port 0/6 goes down, gigabitethernet port 0/8 carries all VLANs of the Flex Link pair.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet0/6    GigabitEthernet0/8    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 0/6 comes up, VLANs preferred on this interface are blocked on the peer interface 0/8 and forwarded on 0/6.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet0/6    GigabitEthernet0/8    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
------------------------------------------------------------------------
GigabitEthernet 0/3 GigabitEthernet 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 (Gi 0/3), 100000 Kbit (Gi0/4)
Mac Address Move Update Vlan : auto
```

### Configuring the MAC Address-Table Move Update Feature

- Configuring a switch to send MAC address-table move updates
- Configuring a switch to get MAC address-table move updates
Chapter 18 Configuring Flex Links and the MAC Address-Table Move Update Feature

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>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</td>
</tr>
<tr>
<td>or</td>
<td>switchport backup interface interface-id mmu primary vlan vlan-id</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>mac address-table move update transmit</td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
</tr>
<tr>
<td>Step 7</td>
<td>show mac address-table move update</td>
</tr>
<tr>
<td>Step 8</td>
<td>copy running-config startup config</td>
</tr>
</tbody>
</table>

To disable the MAC address-table move update feature, 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:

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet0/1
Switch(conf-if)# switchport backup interface gigabitethernet0/2 mmu primary vlan 2
Switch(conf-if)# exit
Switch(conf)# mac address-table move update transmit
Switch(conf)# end
```

This example shows how to verify the configuration:

```
Switch# show mac-address-table move update
Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 5
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
```

**Command Purpose**

**Step 1**

**configure terminal**

Enter global configuration mode.

**Step 2**

**interface interface-id**

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.

**Step 3**

**switchport backup interface interface-id**

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.

**or**

**switchport backup interface interface-id mmu primary vlan vlan-id**

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. When one link is forwarding traffic, the other interface is in standby mode.

**Step 4**

**end**

Return to global configuration mode.

**Step 5**

**mac address-table move update transmit**

Enable the access switch to send MAC address-table move updates to other switches in the network if the primary link goes down and the switch starts forwarding traffic through the standby link.

**Step 6**

**end**

Return to privileged EXEC mode.

**Step 7**

**show mac address-table move update**

Verify the configuration.

**Step 8**

**copy running-config startup config**

(Optional) Save your entries in the switch startup configuration file.
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>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>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></td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>show mac address-table move update</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td></td>
<td>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, 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(conf)# mac address-table move update receive
Switch(conf)# end
```

### Monitoring Flex Links and the MAC Address-Table Move Update

Table 18-1 shows the privileged EXEC command for monitoring Flex Link configuration.

<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 displays all Flex Links configured on the switch 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>
Configuring IGMP Snooping

This chapter describes how to configure Internet Group Management Protocol (IGMP) snooping on the Cisco ME 3800X and ME 3600X switch. It also includes procedures for controlling multicast group membership by using IGMP filtering and procedures for configuring the IGMP throttling action.

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.

- Understanding IGMP Snooping, page 19-1
- Configuring IGMP Snooping, page 19-6
- Displaying IGMP Snooping Information, page 19-13
- Configuring IGMP Filtering and Throttling, page 19-14
- Displaying IGMP Filtering and Throttling Configuration, page 19-19

Note
You can either manage IP multicast group addresses through features such as IGMP snooping, 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.

Note
For more information on IP multicast and IGMP, see RFC 1112 and RFC 2236.
The multicast router 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.

If a port spanning-tree, a port group, or a VLAN ID changes, the IGMP snooping-learned multicast groups from this port on the VLAN are deleted.

These sections describe IGMP snooping characteristics:

- IGMP Support, page 19-2
- IGMP Versions, page 19-3
- Joining a Multicast Group, page 19-3
- Leaving a Multicast Group, page 19-5
- Immediate Leave, page 19-6
- IGMP Configurable-Leave Timer, page 19-6
- IGMP Report Suppression, page 19-6

**IGMP Support**

IGMP snooping is supported over Switch Ports, EVCs, Ethernet over MPLS (EoMPLS), and Virtual Private LAN Services (VPLS) over Pseudowire (PW).

IGMP snooping supports the following:

- configuration of IGMP snooping over EVC interfaces with a single EFP or multiple EFPs per bridge domain.
- L2 multicast deployment on the customer access side of a network. Enabling IGMP snooping on EVCs allows snooping of IGMP requests.

Tags should be popped from a packet before the packet is sent to the IGMP snooping, using the `rewrite ingress tag pop 1/2 symmetric` command.

**Note**

IGMP snooping is not supported on Pseudowire if the core interface is an svi.
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 IGMPv1 switch and the switch receives an IGMPv2 report from a host, the switch can forward the IGMPv2 report to the multicast router.

Note

The switches support IGMPv3 snooping based only on the destination multicast MAC address. They do 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.

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:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtssm5t.htm

Joining a Multicast Group

When a host connected to the switch wants to join an IP multicast group and 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 19-1.
Understanding IGMP Snooping

Router A sends a general query to the switch, which forwards the query to ports 2 through 5, which are 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. The switch CPU uses the information in the IGMP report to set up a forwarding-table entry, as shown in Table 19-1, that includes the port numbers connected to Host 1 and the router.

<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 19-2), the CPU receives that message and adds the port number of Host 4 to the forwarding table as shown in Table 19-2. Note that because the forwarding table directs IGMP messages to only 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.
Chapter 19  Configuring IGMP Snooping

Understanding IGMP Snooping

Figure 19-2  Second Host Joining a Multicast Group

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 and Protocol Independent Multicast (PIM) packets
- Statically connecting to a multicast router port with the `ip igmp snooping mrouter` global configuration command

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 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.

---

Table 19-2  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>
Immediate Leave

Immediate Leave is only supported on IGMP Version 2 hosts.

The switch uses IGMP snooping Immediate Leave 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 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 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 inadvertently be dropped.

For configuration steps, see the “Enabling IGMP Immediate Leave” section on page 19-9.

IGMP Configurable-Leave Timer

You can configure the time that the switch waits after sending a group-specific query to determine if hosts are still interested in a specific multicast group. The IGMP leave response time can be configured from 100 to 5000 milliseconds. The timer can be set either globally or on a per-VLAN basis. The VLAN configuration of the leave time overrides the global configuration.

For configuration steps, see the “Configuring the IGMP Leave Timer” section on page 19-10.

IGMP Report Suppression

Note
IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 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 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 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 19-12.

Configuring IGMP Snooping

IGMP snooping allows switches to examine IGMP packets and make forwarding decisions based on their content.

- Default IGMP Snooping Configuration, page 19-7
Default IGMP Snooping Configuration

Table 19-3  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</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>TCN(^1) flood query count</td>
<td>2</td>
</tr>
<tr>
<td>TCN query solicitation</td>
<td>Disabled</td>
</tr>
<tr>
<td>IGMP report suppression</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

\(^1\) TCN = Topology Change Notification

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>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip igmp snooping</td>
<td>Globally enable IGMP snooping in all existing VLAN interfaces.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</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 globally disable IGMP snooping on all VLAN interfaces, use the **no ip igmp snooping** global configuration command.
Beginning in privileged EXEC mode, follow these steps to enable IGMP snooping on a VLAN 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><code>ip igmp snooping vlan vlan-id</code></td>
<td>Enable IGMP snooping on the VLAN interface. The VLAN ID range is 1 to 1001 and 1006 to 4094. <strong>Note</strong> IGMP snooping must be globally enabled before you can enable VLAN snooping.</td>
</tr>
<tr>
<td>end</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>

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.

---

### 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 mrouter interface interface-id` 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>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| `ip igmp snooping vlan vlan-id mrouter interface interface-id` | Specify the multicast router VLAN ID and the interface to the multicast router.  
- The VLAN ID range is 1 to 1001 and 1006 to 4094.  
- The interface can be a physical interface or a port channel. The port-channel range is 1 to 26. **Note** The switch supports switchport and port channel interfaces. |
| end | Return to privileged EXEC mode. |
| `show ip igmp snooping mrouter [vlan vlan-id]` | Verify that IGMP snooping is enabled on the VLAN interface. |
| `copy running-config startup-config` | (Optional) Save your entries in the configuration file. |

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 gigabitethernet0/2
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:

<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 vlan vlan-id static ip_address 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>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ip igmp snooping groups</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

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 a port:

Switch# configure terminal
Switch(config)# ip igmp snooping vlan 105 static 224.2.4.12 interface gigabitethernet0/1
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 only use the Immediate-Leave feature when there is a single receiver present on every port in the VLAN.

**Note**

Immediate Leave is supported only on 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</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip igmp snooping vlan vlan-id immediate-leave</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
</tbody>
</table>
Configuring IGMP Snooping

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 Leave Timer

Follow these guidelines when configuring the IGMP leave timer:

- You can configure the leave time globally or on a per-VLAN basis.
- Configuring the leave time on a VLAN overrides the global setting.
- The default leave time is 1000 milliseconds.
- The IGMP configurable leave time is only supported on hosts running IGMP Version 2.
- The actual leave latency in the network is usually the configured leave time. However, the leave time might vary around the configured time, depending on real-time CPU load conditions, network delays and the amount of traffic sent through the interface.

Beginning in privileged EXEC mode, follow these steps to enable the IGMP configurable-leave timer:

<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 last-member-query-interval time</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip igmp snooping vlan vlan-id last-member-query-interval time</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show ip igmp snooping</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</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.

Use the `no ip igmp snooping last-member-query-interval` global configuration command to globally reset the IGMP leave timer to the default setting.

Use the `no ip igmp snooping vlan vlan-id last-member-query-interval global configuration command` to remove the configured IGMP leave-time setting from the specified VLAN.
Configuring TCN-Related Commands

These sections describe how to control flooded multicast traffic during a TCN event:

- Controlling the Multicast Flooding Time After a TCN Event, page 19-11
- Recovering from Flood Mode, page 19-11
- Disabling Multicast Flooding During a TCN Event, page 19-12

Controlling the Multicast Flooding Time After a TCN Event

You can control the time that multicast traffic is flooded after a TCH event by using the `ip igmp snooping tcn flood query count` global configuration command. This command configures the number of general queries for which multicast data traffic is flooded after a TCN event. Some examples of TCN events are the client changed its location and the receiver is on same port that was blocked but is now forwarding, and a port went down without sending a leave message.

If you set the TCN flood query count to 1 by using the `ip igmp snooping tcn flood query count` command, the flooding stops after receiving one general query. If you set the count to 7, the flooding of multicast traffic due to the TCN event lasts until 7 general queries are received. Groups are relearned based on the general queries received during the TCN event.

Beginning in privileged EXEC mode, follow these steps to configure the TCN flood query count:

<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 tcn flood query count <code>count</code></td>
<td>Specify the number of IGMP general queries for which the multicast traffic is flooded. The range is 1 to 10. By default, the flooding query count is 2.</td>
</tr>
<tr>
<td>3</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>4</td>
<td>show ip igmp snooping</td>
<td>Verify the TCN settings.</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 flooding query count, use the `no ip igmp snooping tcn flood query count` global configuration command.

Recovering from Flood Mode

When a topology change occurs, the spanning-tree root sends a special IGMP leave message (also known as global leave) with the group multicast address 0.0.0.0. However, when you enable the `ip igmp snooping tcn query solicit` global configuration command, the switch sends the global leave message whether or not it is the spanning-tree root. When the router receives this special leave, it immediately sends general queries, which expedite the process of recovering from the flood mode during the TCN event. Leaves are always sent if the switch is the spanning-tree root regardless of this configuration command. By default, query solicitation is disabled.
Beginning in privileged EXEC mode, follow these steps to enable the switch sends the global leave message whether or not it is the spanning-tree root:

<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 tcn query solicit</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 return to the default query solicitation, use the `no ip igmp snooping tcn query solicit` global configuration command.

### Disabling Multicast Flooding During a TCN Event

When the switch receives a TCN, multicast traffic is flooded to all the ports until two general queries are received. If the switch has many ports with attached hosts that are subscribed to different multicast groups, the flooding might exceed the capacity of the link and cause packet loss. You can use the `ip igmp snooping tcn flood` interface configuration command to control this behavior.

Beginning in privileged EXEC mode, follow these steps to disable multicast flooding 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>no ip igmp snooping tcn flood</td>
</tr>
<tr>
<td>Step 4</td>
<td>exit</td>
</tr>
<tr>
<td>Step 5</td>
<td>show ip igmp snooping</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To re-enable multicast flooding on an interface, use the `ip igmp snooping tcn flood` interface configuration command.

### 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>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>no ip igmp snooping report-suppression</td>
<td>Disable IGMP report suppression.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ip igmp snooping</td>
<td>Verify that IGMP report suppression is disabled.</td>
</tr>
<tr>
<td>Step 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 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 19-4.

<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. |
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. You can also set the maximum number of IGMP groups that a Layer 2 interface can join.

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 IGMP or MVR is used to forward the multicast traffic.
IGMP filtering is applicable only to the dynamic learning of IP multicast group addresses, not static configuration.

With the IGMP throttling feature, you can 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 contain this configuration information:

- Default IGMP Filtering and Throttling Configuration, page 19-15
- Configuring IGMP Profiles, page 19-15 (optional)
- Applying IGMP Profiles, page 19-16 (optional)
- Setting the Maximum Number of IGMP Groups, page 19-17 (optional)
- Configuring the IGMP Throttling Action, page 19-18 (optional)

## Default IGMP Filtering and Throttling Configuration

Table 19-5 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” section on page 19-18.

## 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.
- **exit**: Exits from igmp-profile configuration mode.
- **no**: Negates a command or returns to its defaults.
- **permit**: Specifies that matching addresses are permitted.
- **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>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 profile profile number</td>
</tr>
<tr>
<td>Step 3</td>
<td>permit</td>
</tr>
<tr>
<td>Step 4</td>
<td>range ip multicast address</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Step 6</td>
<td>show ip igmp profile profile number</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config</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 only to Layer 2 access ports; 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 have only one profile applied to it.
Configure IGMP Snooping

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>Specify the physical interface, and enter interface configuration mode. 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 range is 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 gigabitethernet0/2
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 max-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 can use this command on a logical EtherChannel interface but cannot use it on ports that belong to an EtherChannel port group.

Beginning in privileged EXEC mode, follow these steps to set the maximum number of IGMP groups in the forwarding table:

<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 to be configured, and enter interface configuration mode. The interface can be a Layer 2 port that does not belong to an EtherChannel group or a EtherChannel interface.</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 to 25 the number of IGMP groups that a port can join.

```
Switch(config)# interface gigabitethernet0/2
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>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><code>interface interface-id</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>`ip igmp max-groups action {deny</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 19 Configuring IGMP Snooping

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.

This example shows how to configure a port to remove a randomly selected multicast entry in the forwarding table and to add an IGMP group to the forwarding table when the maximum number of entries is in the table.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip igmp max-groups action replace
Switch(config-if)# end
```

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 19-6 to display IGMP filtering and throttling configuration:

<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><code>show running-config interface interface-id</code></td>
<td>Verify the configuration.</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>

### Table 19-6 Commands for Displaying IGMP Filtering and Throttling Configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip igmp profile [profile number]</code></td>
<td>Displays the specified IGMP profile or all the IGMP profiles defined on the switch.</td>
</tr>
<tr>
<td><code>show running-config [interface interface-id]</code></td>
<td>Displays the configuration of the specified interface or the configuration of all interfaces on the switch, including (if configured) the maximum number of IGMP groups to which an interface can belong and the IGMP profile applied to the interface.</td>
</tr>
</tbody>
</table>
Configuring Traffic Control

This chapter describes how to configure the traffic control features on the Cisco ME 3800X and ME 3600X switch.

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

- Configuring Storm Control, page 20-1
- Configuring Port Blocking, page 20-5
- Configuring EVC MAC Security, page 20-6
- Displaying Traffic Control Settings, page 20-12

Configuring Storm Control

- Understanding Storm Control, page 20-1
- Default Storm Control Configuration, page 20-3
- Configuring Storm Control and Threshold Levels, page 20-3

Understanding Storm Control

The Cisco ME 3800X and 3600X switches support storm control on physical interfaces. When you configure storm control on an interface, it also affects traffic on Ethernet Flow Points (EFPs) configured on the interface.

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
- Traffic rate in bits per second at which broadcast, multicast, or unicast packets are received
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 entering an interface 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 20-1 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 20-1 Broadcast Storm Control Example](image)

The combination of the storm-control suppression level and the 200 ms 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.

Note

Because packets do not arrive at uniform intervals, the 1-second 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.

**Note**
Storm control configuration affects traffic on both the switchport and any EVCs on the switchport.

## Default Storm Control Configuration

By default, unicast, broadcast, and multicast storm control are 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.

**Note**
You can configure storm control on physical interfaces or on an EtherChannel. When you configure storm control on an EtherChannel, the storm control settings propagate to the EtherChannel physical interfaces.

Beginning in privileged EXEC mode, follow these steps to storm control and threshold levels:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>interface interface-id</code></td>
<td>Specify the type and number of the physical interface to configure, for example <code>gigabitethernet0/1</code>, and enter interface configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Storm Control

**Step 3**

```bash
storm-control { broadcast | multicast | unicast } level { rising_level [falling_level] | bps bps [bps-low] | pps pps [pps-low] }
```

Configure broadcast, multicast, or unicast storm control. By default, storm control is disabled.

The keywords have these meanings:

- For `rising_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 `falling_level`, 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**.

- 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**

```bash
storm-control action { shutdown | trap }
```

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**

```bash
end
```

Return to privileged EXEC mode.

**Step 6**

```bash
show storm-control [interface-id] [broadcast | multicast | unicast]
```

Verify the storm control suppression levels set on the interface for the specified traffic type. If you do not enter a traffic type, broadcast storm control settings are displayed.

**Step 7**

```bash
copy running-config startup-config
```

(Optional) Save your entries in the configuration file.
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 gigabitethernet0/1
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 gigabitethernet0/1
Switch(config-if)# storm-control broadcast level 20
```

## 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, page 20-5  
- Blocking Flooded Traffic on an Interface, page 20-5

## 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

The interface can be a physical interface or an EtherChannel group. When you block multicast or unicast traffic for a port channel, it is blocked on all ports in the port-channel group.

> **Note**
> You cannot configure port blocking on an interface that has a service instance configured.
Beginning in privileged EXEC mode, follow these steps to disable the flooding of unicast and Layer 2 multicast packets out of 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 to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 switchport block multicast</td>
<td>Block unknown multicast forwarding out of the port.</td>
</tr>
<tr>
<td>Step 4 switchport block unicast</td>
<td>Block unknown unicast forwarding out of the port.</td>
</tr>
<tr>
<td>Step 5 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6 show interfaces interface-id switchport</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 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 a port:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport block multicast
Switch(config-if)# switchport block unicast
Switch(config-if)# end
```

### Configuring EVC MAC Security

You can use the Ethernet Virtual Connection (EVC) MAC security feature to restrict input to an Ethernet flow point (EFP) service instance by limiting and identifying MAC addresses of the stations allowed accessing the EFP. When you assign secure MAC addresses to a secured EFP, the EFP 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 EFP is assured the full bandwidth of the port.

You can enter the mac security maximum addresses service-instance command to configure an upper limit for the number of secure MAC addresses allowed on an EFP, including permitted addresses, dynamically learned addresses, and sticky addresses. If you do not configure an upper limit, the default number of secured MAC addresses is 1.

If an EFP is configured as a secure EFP and the maximum number of secure MAC addresses is reached, when the MAC address of a station attempting to access the EFP 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 EFP attempts to access another secure EFP, a violation is flagged.

These sections contain this conceptual and configuration information:

- Understanding MAC Security, page 20-7
- Default EVC MAC Security Configuration, page 20-8
Understanding MAC Security

- Secure MAC Addresses, page 20-7
- Security Violations, page 20-7

Secure MAC Addresses

You configure the maximum number of secure addresses allowed on an EFP by using the `mac security maximum address value` service instance configuration command.

**Note**

If you try to set the maximum value to a number less than the number of static or sticky secure addresses already configured on a secure EFP, the command is rejected. If the number of static or sticky secure addresses configured on a secure EFP is less than the new maximum value, the command is accepted and dynamic secure addresses may get deleted to satisfy maximum number of secure address.

The switch supports these types of secure MAC addresses:

- Static secure MAC addresses—These are manually configured by using the `mac security address permits mac-address` service instance configuration command. Static secure MAC addresses are stored in the address table and added to the switch running configuration.
- Dynamic secure MAC addresses—These are dynamically learned, 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 service instance does not need to dynamically reconfigure them.

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 removed from both address table and the running configuration.

You can set the maximum number of secure MAC addresses that you can configure on a bridge domain is determined by using the `mac limit max addresses` bridge-domain configuration command. The range is 1 to 10000.

Security Violations

It is a security violation when one of these situations occurs:

- The maximum number of secure MAC addresses for a secure EFP have been added to the address table, and a station whose MAC address is not in the address table attempts to access the EFP.
- An address learned or configured on one secure EFP is seen on another secure EFP in the same bridge domain.
You can configure the EFP 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 EFP, 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 maximum limit allowed on the EFP, 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 MAC security violation causes the EFP service instance to become error-disabled and to shut down immediately. An SNMP trap is sent, a syslog message is logged, and the violation counter increments. When a secure EFP is in the error-disabled state, you can manually re-enable it using `clear ethernet service instance number` `interface` `interface-id` privileged EXEC command or entering the **shutdown** and **no shutdown** service instance configuration commands. This is the default mode.

Table 20-1 shows the violation mode and the actions taken when you configure a secure EFP.

### Table 20-1 Security Violation Mode Actions

<table>
<thead>
<tr>
<th>Violation Mode</th>
<th>Traffic is forwarded</th>
<th>Sends SNMP trap</th>
<th>Sends syslog message</th>
<th>Displays error message</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 EVC MAC Security Configuration

### Table 20-2 Default EVC MAC Security Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVC MAC security</td>
<td>Disabled on an EFP.</td>
</tr>
<tr>
<td>Sticky address learning</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Maximum number of secure MAC addresses per EFP</td>
<td>1.</td>
</tr>
<tr>
<td>Violation mode</td>
<td>Shutdown. The service instance shuts down when the maximum number of secure MAC addresses is exceeded.</td>
</tr>
<tr>
<td>MAC security aging</td>
<td>Disabled. Aging time is 0. Static aging is disabled.</td>
</tr>
</tbody>
</table>
MAC Address Security Guidelines

- MAC security is disabled by default on an EFP. When MAC security is disabled on an EFP, you can configure MAC security functions, but they do not become operational until you enable MAC security.
  - A secured EFP is one on which MAC security is enabled.
  - A secured MAC address is one that is configured or learned.
  - A secured bridge domain is one on which MAC security is enabled.
- Secured EFP learned MAC addresses are kept in both the EVC MAC security table and the system MAC address table. Secured addresses are aged out by the configured MAC security aging process.
- When you enable MAC security on an EFP by entering the `mac security service-instance` configuration command, the existing MAC addresses on the EFP that were dynamically learned are removed, and configured MAC addresses and sticky MAC address entries are added to the EVC MAC security table.
- When you remove an EFP from a bridge domain or move an EFP to a new bridge domain, all MAC addresses for the EFP are removed from the MAC address table.
- A MAC locking condition occurs when a MAC move occurs and a MAC entry already exists for an EFP in a given bridge domain, and the same MAC address is received on a different EFP in the bridge domain. If the move takes place from one secured EFP to another secured EFP, the move is not allowed and the configured violation action occurs. A move between a secured and non-secured EFP is allowed because no violation occurs.

Enabling and Configuring EVC MAC Security

For detailed information about the commands, see the Cisco IOS Carrier Ethernet Command Reference at:


Beginning in privileged EXEC mode, follow these steps to configure MAC security on an EFP:

<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 <code>interface-id</code></td>
<td>Specify the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport mode trunk</td>
<td>Configure the interface as a trunk port, required for EFP configuration.</td>
</tr>
<tr>
<td>Step 4</td>
<td>switchport trunk allowed vlan</td>
<td>Configure the interface to have no allowed VLANs.</td>
</tr>
<tr>
<td></td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>service instance <code>number ethernet [name]</code></td>
<td>Configure an EFP (service instance) and enter service instance configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The <code>number</code> is the EFP identifier, an integer from 1 to 4000.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) <code>ethernet name</code> is the name of a previously configured Ethernet virtual connection (EVC). You do not need to use an EVC name in a service instance.</td>
</tr>
</tbody>
</table>
## Configuring EVC MAC Security

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>encapsulation {default</td>
<td>dot1q</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• default—Configure to match all unmatched packets.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• dot1q—Configure 802.1Q encapsulation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• priority-tagged—Specify priority-tagged frames, VLAN-ID 0 and CoS value of 0 to 7.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• untagged—Map to untagged VLANs. Only one EFP per port can have untagged encapsulation.</td>
</tr>
<tr>
<td></td>
<td>Note</td>
<td>You must configure encapsulation before you can configure a bridge domain. You must configure a bridge domain to be able to configure some MAC security commands.</td>
</tr>
<tr>
<td>Step 7</td>
<td>bridge-domain bridge-id [split-horizon group group-id]</td>
<td>Configure the bridge domain ID. The range is from 1 to 8000.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) split-horizon group group-id—Configure a split-horizon group. The group ID is from 1 to 3. EFPs in the same bridge domain and split-horizon group cannot forward traffic between each other, but can forward traffic between other EFPs in the same bridge domain but not in the same split-horizon group.</td>
</tr>
<tr>
<td></td>
<td>Note</td>
<td>You must configure a bridge domain to see the mac security aging static command or to configure a MAC security maximum address value of more than one.</td>
</tr>
<tr>
<td>Step 8</td>
<td>mac security</td>
<td>Enable MAC security on the EFP.</td>
</tr>
<tr>
<td>Step 9</td>
<td>mac security address {permit</td>
<td>deny} mac-address</td>
</tr>
<tr>
<td>Step 10</td>
<td>mac security maximum addresses value</td>
<td>(Optional) Set the maximum number of secure MAC addresses allowed on the service instance. The range is 1 to 1000. Entering a value of 0 disables dynamic MAC address learning. The maximum number of secure MAC addresses on an EFP is 1000. The maximum number on a bridge domain or on a switch depends on the feature license.</td>
</tr>
<tr>
<td>Step 11</td>
<td>mac security violation {protect</td>
<td>restrict}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>
Chapter 20  Configuring Traffic Control

Configuring EVC MAC Security

Use the no form of the commands to remove the configuration and return to the default configuration.

This example shows how to enable mac security on a service instance, permit the specified MAC address, and to set the maximum number of secure addresses to 50. MAC security aging time is 750 minutes. The violation mode is the default (errdisable) and sticky learning is enabled.

Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport mode allowed VLAN none
Switch (config-if)# service instance 2 Ethernet
Switch (config-if-srv)# encapsulation dot1q
Switch (config-if-srv)# bridge-domain 2
Switch (config-if-srv)# mac security
Switch (config-if-srv)# mac security permit mac-address 0000.0000.0003
Switch (config-if-srv)# mac security maximum addresses 50
Switch (config-if-srv)# mac security aging time 750
Switch (config-if-srv)# mac security sticky
Switch (config-if-srv)# end

You can verify the previous commands by entering the show ethernet service instance number interface interface-id mac security privileged EXEC command.
## Displaying Traffic Control Settings

### Table 20-3 Commands for Displaying Traffic Control Status and Configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show ethernet service instance number interface-id mac security</strong></td>
<td>Displays information about MAC security configured on the service instance.</td>
</tr>
<tr>
<td><strong>show interfaces [interface-id] switchport</strong></td>
<td>Displays the administrative and operational status of all switching (nonrouting) ports or the specified port, including port blocking settings.</td>
</tr>
<tr>
<td>**show storm-control [interface-id] [broadcast</td>
<td>multicast</td>
</tr>
</tbody>
</table>
CHAPTER 21

Configuring CDP

This chapter describes how to configure Cisco Discovery Protocol (CDP) on the Cisco ME 3800X and ME 3600X switch.

Note: 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.

- Understanding CDP, page 21-1
- Configuring CDP, page 21-2
- Monitoring and Maintaining CDP, page 21-5

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.

The switch supports CDP Version 2.
Configuring CDP

- Default CDP Configuration, page 21-2
- Configuring the CDP Characteristics, page 21-2
- Disabling and Enabling CDP, page 21-3
- Disabling and Enabling CDP on an Interface, page 21-4
- CDP and Ethernet Flow Points (EFPs), page 21-4

Default CDP Configuration

Table 21-1 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 only on NNIs; disabled on ENIs Note CDP is not supported on UNIs.</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</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>cdp timer seconds                                                      (Optional) Set the transmission frequency of CDP updates in seconds. The range is 5 to 254; the default is 60 seconds.</td>
</tr>
<tr>
<td>Step 3</td>
<td>cdp holdtime seconds                                                  (Optional) Specify the amount of time a receiving device should hold the information sent by your device before discarding it. The range is 10 to 255 seconds; the default is 180 seconds.</td>
</tr>
<tr>
<td>Step 4</td>
<td>cdp advertise-v2                                                       (Optional) Configure CDP to send Version-2 advertisements. This is the default state.</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Use the **no** form of the CDP commands to return to the default settings.

This example shows how to configure CDP characteristics.

```sh
Switch# configure terminal
Switch(config)# cdp timer 50
Switch(config)# cdp holdtime 120
Switch(config)# cdp advertise-v2
Switch(config)# end
```

For additional CDP **show** commands, see the “Monitoring and Maintaining CDP” section on page 21-5.

### Disabling and Enabling CDP

CDP is enabled by default.

**Note**

Cisco devices (such as Cisco IP Phones) regularly exchange CDP messages with connected devices. Disabling CDP can interrupt device connectivity.

Beginning in privileged EXEC mode, follow these steps to globally disable the CDP device discovery capability:

<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> no cdp run</td>
<td>Disable CDP.</td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Beginning in privileged EXEC mode, follow these steps to globally enable CDP when it has been disabled:

<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> cdp run</td>
<td>Enable CDP after disabling it.</td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

This example shows how to globally enable CDP if it has been disabled.

```sh
Switch# configure terminal
Switch(config)# cdp run
Switch(config)# end
```
Disabling and Enabling CDP on an Interface

CDP is enabled by default to send and to receive CDP information.

Beginning in privileged EXEC mode, follow these steps to disable CDP on a 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>Specify the interface on which you are disabling CDP, and enter interface configuration mode. CDP is enabled by default.</td>
</tr>
<tr>
<td>Step 3 no cdp enable</td>
<td>Disable CDP on the 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 a port 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>Specify the interface on which you are enabling CDP, and enter interface configuration mode. CDP is enabled by default.</td>
</tr>
<tr>
<td>Step 3 cdp enable</td>
<td>Enable CDP on the 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 gigabitethernet0/1
Switch(config-if)# cdp enable
Switch(config-if)# end

CDP and Ethernet Flow Points (EFPs)

For CDP to peer with a neighbor on a port that has an Ethernet Virtual Connection (EVC) EFP service instance configured, you need to enter the 12 protocol peer cdp service-instance configuration command on the service instance. See the “Configuring Ethernet Virtual Connections (EVCs)” chapter for more information on EFPs.
This example shows how to configure Layer 2 protocol peer on a service instance:

```
Switch (config)# interface gigabitethernet0/1
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan none
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation untagged
Switch (config-if-srv)# l2protocol peer cdp
Switch (config-if-srv)# bridge-domain 10
Switch (config-if-srv)# end
```

## Monitoring and Maintaining CDP

To monitor and maintain CDP on your device, use one or more of these commands in privileged EXEC mode.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear cdp counters</td>
<td>Reset the traffic counters to zero.</td>
</tr>
<tr>
<td>clear cdp table</td>
<td>Delete the CDP table of information about neighbors.</td>
</tr>
<tr>
<td>show cdp</td>
<td>Display global information, such as frequency of transmissions and the holdtime for packets being sent.</td>
</tr>
<tr>
<td>show cdp entry entry-name [protocol</td>
<td>version]</td>
</tr>
<tr>
<td>show cdp interface [interface-id]</td>
<td>Display information about interfaces where CDP is enabled. You can limit the display to the interface about which you want information.</td>
</tr>
<tr>
<td>show cdp neighbors [interface-id] [detail]</td>
<td>Display information about neighbors, including device type, interface type and number, holdtime settings, capabilities, platform, and port ID. You can limit the display to neighbors of a specific interface or expand the display to provide more detailed information.</td>
</tr>
<tr>
<td>show cdp traffic</td>
<td>Display CDP counters, including the number of packets sent and received and checksum errors.</td>
</tr>
</tbody>
</table>
CHAPTER 22

Configuring LLDP and LLDP-MED

This chapter describes how to configure the Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED) on the Cisco ME 3800X and ME 3600X switch.

Understanding LLDP and LLDP-MED

- Understanding LLDP, page 22-1
- Understanding LLDP-MED, page 22-2

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.

By default, LLDP is disabled globally and on interfaces.
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)

### 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

- Default LLDP Configuration, page 22-3
- Configuring LLDP Characteristics, page 22-3
- Disabling and Enabling LLDP Globally, page 22-4
- Disabling and Enabling LLDP on an Interface, page 22-5
- Configuring LLDP-MED TLVs, page 22-6
- LLDP and Ethernet Flow Points (EFPs), page 22-7

### Default LLDP Configuration

Table 22-1 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>Enabled</td>
</tr>
<tr>
<td>LLDP transmit</td>
<td>Enabled</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><strong>Step 2</strong> lldp holdtime</td>
<td><strong>seconds</strong> (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> lldp reinit</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> lldp timer</td>
<td><strong>seconds</strong> (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> lldp tlv-select</td>
<td>(Optional) Specify the LLDP TLVs to send or receive.</td>
</tr>
<tr>
<td><strong>Step 6</strong> lldp med-tlv-select</td>
<td>(Optional) Specify the LLDP-MED TLVs to send or receive.</td>
</tr>
<tr>
<td><strong>Step 7</strong> copy running-config</td>
<td>startup-config (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 22-7.

### Disabling and Enabling LLDP Globally

By default LLDP is disabled globally and on interfaces.

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><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong> no lldp run</td>
<td>Disable LLDP.</td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Return to privileged EXEC mode.</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>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>lldp run</td>
<td>Enable LLDP.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</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**

By default, when LLDP is enabled, interfaces are enabled to send and to receive LLDP information. Beginning in privileged EXEC mode, follow these steps to disable sending or receiving LLDP packets on an 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 interface-id</td>
<td>Specify the interface on which you are disabling LLDP, and enter interface configuration mode.</td>
</tr>
<tr>
<td>no lldp transmit</td>
<td>No LLDP packets are sent on the interface.</td>
</tr>
<tr>
<td>no lldp receive</td>
<td>No LLDP packets are received on the interface.</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>

Beginning in privileged EXEC mode, follow these steps to enable sending and receiving LLDP packets on an interface after it has been disabled:

<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 interface on which you are enabling LLDP, and enter interface configuration mode.</td>
</tr>
<tr>
<td>lldp transmit</td>
<td>LLDP packets are sent on the interface.</td>
</tr>
<tr>
<td>lldp receive</td>
<td>LLDP packets are received on the interface.</td>
</tr>
</tbody>
</table>
Chapter 22 Configuring LLDP and LLDP-MED

Configuring LLDP and LLDP-MED

This example shows how to enable sending and receiving LLDP packets 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.

Using the `lldp` interface configuration command, you can configure the interface not to send the TLVs listed in Table 22-2.

### Table 22-2 LLDP-MED TLVs

<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>
</tbody>
</table>
**Chapter 22  Configuring LLDP and LLDP-MED**

### 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>
<tr>
<td>show lldp entry entry-name</td>
<td>Display information about a specific neighbor.</td>
</tr>
<tr>
<td>show lldp interface [interface-id]</td>
<td>Display information about interfaces where LLDP is enabled.</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
```

### LLDP and Ethernet Flow Points (EFPs)

For LLDP to peer with a neighbor on a port that has an Ethernet Virtual Connection (EVC) EFP service instance configured, you need to enter the `l2 protocol peer lldp` service-instance configuration command on the service instance. See the “Configuring Ethernet Virtual Connections (EVCs)” chapter for more information on EFPs.

This example shows how to configure Layer 2 protocol peer on a service instance:

```
Switch (config)# interface gigabitEthernet0/1
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan none
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation untagged
Switch (config-if-srv)# l2protocol peer lldp
Switch (config-if-srv)# bridge-domain 10
Switch (config-if-srv)# 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.
### Monitoring and Maintaining LLDP and LLDP-MED

#### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show lldp neighbors [interface-id] [detail]</td>
<td>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.</td>
</tr>
<tr>
<td>show lldp traffic</td>
<td>Display LLDP counters, including the number of packets sent and received, number of packets discarded, and number of unrecognized TLVs.</td>
</tr>
</tbody>
</table>
Configuring UDLD

This chapter describes how to configure the UniDirectional Link Detection (UDLD) protocol on the Cisco ME 3800X and 3600X switch.

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

- Understanding UDLD, page 23-1
- Configuring UDLD, page 23-3
- Displaying UDLD Status, page 23-7

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 disables the affected port 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 can also detect unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and to misconnected ports on fiber-optic links.

In normal and aggressive modes, 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 ports. 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.
Understanding UDLD

In normal mode, UDLD detects 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 port.

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 detects 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 detects a unidirectional link by using the previous detection methods. UDLD in aggressive mode can also detect a unidirectional link on a point-to-point link on which no failure between the two devices is allowed. It can also detect a unidirectional link when one of these problems exists:

- On fiber-optic or twisted-pair links, one of the ports cannot send or receive traffic.
- On fiber-optic or twisted-pair links, one of the ports is down while the other is up.
- One of the fiber strands in the cable is disconnected.

In these cases, UDLD disables the affected port.

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 fiber strands in a cable are working normally from a Layer 1 perspective, UDLD in aggressive mode detects whether those fiber strands 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 port 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 a port is disabled and UDLD is running, whenever UDLD is disabled on a port, or whenever the switch is reset, UDLD clears all existing cache entries for the ports 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 be shut down. When UDLD is in aggressive mode, the link is considered unidirectional, and the port is disabled.

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 a port 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 port if, after the fast train of messages, the link state is still undetermined.

Figure 23-1 shows an example of a unidirectional link condition.

**Figure 23-1  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

- Default UDLD Configuration, page 23-4
- Configuration Guidelines, page 23-4
- Enabling UDLD Globally, page 23-5
- Enabling UDLD on an Interface, page 23-5
- Resetting an Interface Disabled by UDLD, page 23-6
- UDLD and Ethernet Flow Points (EFPs), page 23-6
Default UDLD Configuration

Table 23-1 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>

**Configuration Guidelines**

- A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port 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>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>udld { aggressive</td>
<td>enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show udld</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</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 a 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>Specify the port to be enabled for UDLD, and enter interface configuration mode.</td>
</tr>
</tbody>
</table>
Chapter 23  Configuring UDLD

Configuring UDLD

Resetting an Interface Disabled by UDLD

Beginning in privileged EXEC mode, follow these steps to reset all ports disabled by UDLD:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>udld port [aggressive]</td>
</tr>
<tr>
<td></td>
<td>• udld port — Enables UDLD in normal mode on the specified port.</td>
</tr>
<tr>
<td></td>
<td>• udld port aggressive — Enables UDLD in aggressive mode on the specified port.</td>
</tr>
<tr>
<td>Note</td>
<td>Use the no udld port interface configuration command to disable UDLD on a specified fiber-optic port.</td>
</tr>
<tr>
<td></td>
<td>For more information about aggressive and normal modes, see the “Modes of Operation” section on page 23-1.</td>
</tr>
</tbody>
</table>

| Step 4  | end | Return to privileged EXEC mode. |
| Step 5  | show udld interface-id | Verify your entries. |
| Step 6  | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

UDLD and Ethernet Flow Points (EFPs)

For UDLD to peer with a neighbor on a port that has an Ethernet Virtual Connection (EVC) EFP service instance configured, you need to enter the 12 protocol peer udld service-instance configuration command on the service instance. See the “Configuring Ethernet Virtual Connections (EVCs)” chapter for more information on EFPs.
This example shows how to configure Layer 2 protocol peer on a service instance:

Switch (config)# interface gigabitethernet0/1
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan none
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation untagged
Switch (config-if-srv)# l2protocol peer udld
Switch (config-if-srv)# bridge-domain 10
Switch (config-if-srv)# end

Displaying UDLD Status

To display the UDLD status for the specified port or for all ports, use the show udld [interface-id] privileged EXEC command.

For detailed information about the fields in the command output, see the command reference for this release.
Displaying UDLD Status
CHAPTER 24

Configuring System Message Logging

This chapter describes how to configure system message logging on the Cisco ME 3800X and ME 3600X 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.

- Understanding System Message Logging, page 24-1
- Configuring System Message Logging, page 24-2
- Displaying the Logging Configuration, page 24-13

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 appear 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.
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

- System Log Message Format, page 24-2
- Default System Message Logging Configuration, page 24-3
- Disabling Message Logging, page 24-3 (optional)
- Setting the Message Display Destination Device, page 24-4 (optional)
- Synchronizing Log Messages, page 24-5 (optional)
- Enabling and Disabling Time Stamps on Log Messages, page 24-7 (optional)
- Enabling and Disabling Sequence Numbers in Log Messages, page 24-7 (optional)
- Defining the Message Severity Level, page 24-8 (optional)
- Limiting Syslog Messages Sent to the History Table and to SNMP, page 24-9 (optional)
- Enabling the Configuration-Change Logger, page 24-10 (optional)
- Configuring UNIX Syslog Servers, page 24-11 (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 appear in this format:

```
seq no:timestamp: %facility-severity-MNEMONIC:description
```

The part of the message preceding the percent sign depends on the setting of the `service sequence-numbers`, `service timestamps log datetime`, `service timestamps log datetime [localtime]` `[msec] [show-timezone]`, or `service timestamps log uptime` global configuration command.

<table>
<thead>
<tr>
<th>Table 24-1 System Log Message Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Element</td>
</tr>
<tr>
<td><code>seq no:</code></td>
</tr>
<tr>
<td><code>timestamp formats:</code></td>
</tr>
<tr>
<td><code>facility</code></td>
</tr>
</tbody>
</table>
Configuring System Message Logging

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 GigabitEthernet0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
18:47:02: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down
18:48:50.483 UTC: %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 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

Default System Message Logging Configuration

Table 24-2 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 24-3 on page 24-9).</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>Time stamps</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 24-4 on page 24-13).</td>
</tr>
<tr>
<td>Server severity</td>
<td>Informational (and numerically lower levels; see Table 24-3 on page 24-9).</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.

<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 logging console</td>
<td>Disable message logging.</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></td>
</tr>
<tr>
<td>show logging</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>

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 appear 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 24-5.

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.

<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>logging buffered [size]</td>
<td>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 fails, the log file is lost unless you previously saved it to Flash memory. See Step 4. <strong>Note</strong> Do not make the buffer size too large because the switch could run out of memory for other tasks. Use the <code>show memory</code> 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.</td>
</tr>
</tbody>
</table>
Chapter 24 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 is 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 appear, the console again displays the user prompt.

Beginning in privileged EXEC mode, follow these steps to configure synchronous logging. This procedure is optional.

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.

<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** | `line [console | vty] line-number [ending-line-number]` | Specify the line to be configured for synchronous logging of messages.  
- Use the `console` keyword for configurations that occur through the switch console port.  
- Use the `line vty line-number` 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.  
You can change the setting of all 16 vty lines at once by entering:  
`line vty 0 15`  
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:  
`line vty 2`  
When you enter this command, the mode changes to line configuration. |
| **Step 3** | `logging synchronous [level severity-level | all] [limit number-of-buffers]` | Enable synchronous logging of messages.  
- (Optional) For `level severity-level`, specify the message severity level. Messages with a severity level equal to or higher than this value are printed asynchronously. Low numbers mean greater severity and high numbers mean lesser severity. The default is 2.  
- (Optional) Specifying `level all` means that all messages are printed asynchronously regardless of the severity level.  
- (Optional) For `limit number-of-buffers`, 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. |
| **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. |
Enabling and Disabling Time Stamps 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>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>service timestamps log uptime</td>
<td>Enable log time stamps.</td>
</tr>
<tr>
<td>or</td>
<td>The first command enables time stamps on log messages, showing the time since the system was rebooted.</td>
</tr>
<tr>
<td>service timestamps log datetime [msec] [localtime] [show-timezone]</td>
<td>The second command enables time stamps on log messages. Depending on the options selected, the time stamp can include the date, time in milliseconds relative to the local time-zone, and the time zone name.</td>
</tr>
</tbody>
</table>

Step 3  
end  
Return to privileged EXEC mode.

Step 4  
show running-config  
Verify your entries.

Step 5  
copy running-config startup-config  
(Optional) Save your entries in the configuration file.

To disable 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 time stamp, you can display messages with sequence numbers so that you can unambiguously see 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>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>service sequence-numbers</td>
<td>Enable sequence numbers.</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 sequence numbers, use the no service sequence-numbers global configuration command.
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 24-3.

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>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>logging console level</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>logging monitor level</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>logging trap level</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show running-config or show logging</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

**Note**

Specifying a level causes messages at that level and numerically lower levels to appear 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 24-3 describes the level keywords. It also lists the corresponding UNIX syslog definitions from the most severe level to the least severe level.
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.

### 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 24-3 on page 24-9) 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>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>logging history level</td>
<td>Change the default level of syslog messages stored in the history file and sent to the SNMP server.</td>
</tr>
<tr>
<td></td>
<td>See Table 24-3 on page 24-9 for a list of level keywords.</td>
</tr>
<tr>
<td></td>
<td>By default, warnings, errors, critical, alerts, and emergencies messages are sent.</td>
</tr>
</tbody>
</table>
Chapter 24  Configuring System Message Logging

Configuring System Message Logging

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 reenable 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 12.4 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><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> archive</td>
<td>Enter archive configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> log config</td>
<td>Enter configuration-change logger configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> logging enable</td>
<td>Enable configuration change logging.</td>
</tr>
<tr>
<td><strong>Step 5</strong> 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.</td>
</tr>
</tbody>
</table>

**Note** When the configuration log is full, the oldest log entry is removed each time a new entry is entered.
Chapter 24 Configuring System Message Logging

Configuring System Message Logging

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 radius
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:

1. Add a line such as the following to the file /etc/syslog.conf:
   ```
   local7.debug /usr/adm/logs/cisco.log
   ```
Configuring System Message Logging

The `local7` keyword specifies the logging facility to be used; see Table 24-4 on page 24-13 for information on the facilities. The `debug` keyword specifies the syslog level; see Table 24-3 on page 24-9 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:

```bash
$ touch /var/log/cisco.log
$ chmod 666 /var/log/cisco.log
```

**Step 3** Make sure the syslog daemon reads the new changes:

```bash
$ 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></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>logging host</code></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 this command more than once.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>logging trap level</code></td>
<td>Limit messages logged to the syslog servers.</td>
</tr>
<tr>
<td></td>
<td>Be default, syslog servers receive informational messages and lower. See Table 24-3 on page 24-9 for level keywords.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>logging facility facility-type</code></td>
<td>Configure the syslog facility. See Table 24-4 on page 24-13 for facility-type keywords.</td>
</tr>
<tr>
<td></td>
<td>The default is <code>local7</code>.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 7</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 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 24-4 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 24-4    Logging Facility-Type Keywords

<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 \texttt{show logging} privileged EXEC command. For information about the fields in this display, see the \textit{Cisco IOS Configuration Fundamentals Command Reference, Release 12.2}. 
CHAPTER 25

Configuring SNMP

This chapter describes how to configure the Simple Network Management Protocol (SNMP) on the Cisco ME 3800X and ME 3600X switch.

---

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

---

- Understanding SNMP, page 25-1
- Configuring SNMP, page 25-6
- Displaying SNMP Status, page 25-23

---

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 TCP connection, loss of connection to a neighbor, or other significant events.

Although the switch does not support the Cisco Data Collection MIB, 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.
SNMP Versions

This software release supports these SNMP versions:

- **SNMPv1**—The Simple Network Management Protocol, a Full Internet Standard, defined in RFC 1157.
- **SNMPv2C** replaces the Party-based Administrative and Security Framework of SNMPv2Classic with the community-string-based Administrative Framework of SNMPv2C while retaining the bulk retrieval and improved error handling of SNMPv2Classic. It has these features:
  - **SNMPv2**—Version 2 of the Simple Network Management Protocol, a Draft Internet Standard, defined in RFCs 1902 through 1907.
  - **SNMPv2C**—The community-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 cryptographic (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 25-1 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) or Secure Hash Algorithm (SHA)</td>
<td>No</td>
<td>Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.</td>
</tr>
</tbody>
</table>
| SNMPv3      | authPriv (requires the cryptographic software image) | MD5 or SHA | Data Encryption Standard (DES) or Advanced Encryption Standard (AES) | Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Allows specifying the User-based Security Model (USM) with these encryption algorithms:  
  • DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.  
  • 3DES 168-bit encryption  
  • AES 128-bit, 192-bit, or 256-bit encryption |

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, SNMPv2C, or SNMPv3.

### SNMP Manager Functions

The SNMP manager uses information in the MIB to perform the operations described in Table 25-2.

<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.¹</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

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 25-1, 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.

Figure 25-1  **SNMP Network**

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 ifIndex MIB Object Values

In an NMS, the IF-MIB generates and assigns an interface index (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 ifIndex value of 10003, this value is the same after the switch reboots.

The switch uses one of the values in Table 25-3 to assign an ifIndex value to an interface:

**Table 25-3 ifIndex Values**

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>ifIndex Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVI¹</td>
<td>1–4999</td>
</tr>
<tr>
<td>EtherChannel</td>
<td>5000–5012</td>
</tr>
<tr>
<td>Loopback</td>
<td>5013–5077</td>
</tr>
<tr>
<td>Tunnel</td>
<td>5078–5142</td>
</tr>
<tr>
<td>Physical (such as Gigabit Ethernet or SFP²-module interfaces)</td>
<td>10000–14500</td>
</tr>
<tr>
<td>Null</td>
<td>14501</td>
</tr>
</tbody>
</table>

1. SVI = switch virtual interface
2. SFP = small form-factor pluggable

**Note**

The switch might not use sequential values within a range.
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 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

- Default SNMP Configuration, page 25-7
- SNMP Configuration Guidelines, page 25-7
- Disabling the SNMP Agent, page 25-8
- Configuring Community Strings, page 25-8
- Configuring SNMP Groups and Users, page 25-10
- Configuring SNMP Notifications, page 25-12
- Setting the Agent Contact and Location Information, page 25-17
- Limiting TFTP Servers Used Through SNMP, page 25-17
- Configuring MIB Data Collection and Transfer, page 25-18
- Configuring the Cisco Process MIB CPU Threshold Table, page 25-20
- Configuring MIB Data Collection and Transfer, page 25-18
### Default SNMP Configuration

#### Table 25-4  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

If the switch starts and the switch startup configuration has at least one snmp-server global configuration command, the SNMP agent is enabled.

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. See the Cisco IOS Configuration Fundamentals Command Reference for information about when you should configure notify views.

- 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 username 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>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>no snmp-server</td>
<td>Disable the SNMP agent operation.</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>

The `no snmp-server` global configuration command disables all running versions (Version 1, Version 2C, and Version 3) on the device. No specific Cisco 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>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| **snmp-server community** string [view view-name] [ro | rw] [access-list-name or 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. |
| 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. |
| end | Return to privileged EXEC mode. |
| show running-config | Verify your entries. |
| 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</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>snmp-server engineID {local engineid-string</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 25 Configuring SNMP

### Step 3

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| ```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`—Enables 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 cryptographic 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.
Chapter 25      Configuring SNMP

Configuring SNMP

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 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] | v3 [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 EXEC command.

**Step 7**

```plaintext
copy running-config startup-config
```

(Optional) Save your entries in the configuration file.
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` global configuration command to specify whether to send SNMP notifications as traps or informs.

Table 25-5 describes the supported switch traps (notification types). You can enable any or all of these traps and configure a trap manager to receive them.

<table>
<thead>
<tr>
<th>Notification Type Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alarms</td>
<td>Generates alarm traps.</td>
</tr>
<tr>
<td>auth-framework</td>
<td>Generates SNMP CISCO-AUTH-FRAMEWORK-MIB traps.</td>
</tr>
<tr>
<td>bgp</td>
<td>Generates Border Gateway Protocol (BGP) state change traps.</td>
</tr>
<tr>
<td>bridge</td>
<td>Generates STP bridge MIB traps.</td>
</tr>
<tr>
<td>config</td>
<td>Generates a trap for SNMP configuration changes.</td>
</tr>
<tr>
<td>config-copy</td>
<td>Generates a trap for SNMP configuration copy 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>config</td>
<td>Generates a trap for SNMP configuration changes.</td>
</tr>
<tr>
<td>eigrp</td>
<td>Generates a trap for SNMP EIGRP changes.</td>
</tr>
<tr>
<td>envmon</td>
<td>Generates environmental monitor traps. You can enable any or all of these environmental traps: fan, shutdown, status, supply, temperature.</td>
</tr>
<tr>
<td>ethernet-cfm</td>
<td>Generates an SNMP Ethernet CFM trap.</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>mpls-fast-reroute</td>
<td>Generates a trap for MPLS traffic engineering fast reroutes.</td>
</tr>
<tr>
<td>mpls-idp</td>
<td>Generates a trap for MPLS label distribution protocol changes.</td>
</tr>
<tr>
<td>mpls-traffic-eng</td>
<td>Generates a trap for MPLS traffic engineering changes.</td>
</tr>
<tr>
<td>mpls-vpn</td>
<td>Generates a trap for MPLS Virtual Private Network (VPN) changes.</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>rtr</td>
<td>Generates a trap for the SNMP Response Time Reporter (RTR).</td>
</tr>
<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>
</tbody>
</table>
Chapter 25  Configuring SNMP

Configuring SNMP

Note

Though visible in the command-line help strings, the fru-ctrl and vtp keywords are not supported. The snmp-server enable informs global configuration command is not supported. To enable the sending of SNMP inform notifications, use the snmp-server enable traps global configuration command combined with the snmp-server host host-addr informs global configuration command.

You can use the snmp-server host global configuration command to a specific host to receive the notification types listed in Table 25-5.

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

<table>
<thead>
<tr>
<th>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 remote ip-address</td>
<td>Specify the engine ID for the remote host.</td>
</tr>
<tr>
<td>Step 3 snmp-server user username groupname [remote host [udp-port port]]</td>
<td>Configure an SNMP user to be associated with the remote host created in Step 2.</td>
</tr>
<tr>
<td></td>
<td>Note You cannot configure a remote user for an address without first configuring the engine ID for the remote host. Otherwise, you receive an error message, and the command is not executed.</td>
</tr>
<tr>
<td>Step 4 snmp-server group groupname [v1</td>
<td>v2c</td>
</tr>
</tbody>
</table>
### Command Line Interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 5  | `snmp-server host host-addr
        [informs | traps] [version {1 | 2c | 3
        {auth | noauth | priv } ]]
        community-string [notification-type]` | Specify the recipient of an SNMP trap operation.                        |
|         |                                              | - For `host-addr`, specify the name or Internet address of the host (the  |
|         |                                              | targeted recipient).                                                   |
|         |                                              | - (Optional) Enter `informs` to send SNMP informs to the host.           |
|         |                                              | - (Optional) Enter `traps` (the default) to send SNMP traps to the host. |
|         |                                              | - (Optional) Specify the SNMP `version` (1, 2c, or 3). SNMPv1 does        |
|         |                                              |   not support informs.                                                 |
|         |                                              | - (Optional) For Version 3, select authentication level `auth`, `noauth`, |
|         |                                              |   or `priv`.                                                           |
|         | Note                                         | - The `priv` keyword is available only when the cryptographic software   |
|         |                                              |   image is installed.                                                  |
|         |                                              | - For `community-string`, when `version 1` or `version 2c` is specified, |
|         |                                              |   enter the password-like community string sent with the notification    |
|         |                                              |   operation. When `version 3` is specified, enter the SNMPv3 username.  |
|         |                                              | - The `@` symbol is used for delimiting the context information. Avoid  |
|         |                                              |   using the `@` symbol as part of the SNMP community string when         |
|         |                                              |   configuring this command.                                            |
|         |                                              | - (Optional) For `notification-type`, use the keywords listed in Table   |
|         |                                              |   25-5 on page 25-13. If no type is specified, all notifications are     |
|         |                                              |   sent.                                                                |
| Step 6  | `snmp-server enable traps
        notification-types` | 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  |
|         |                                              |   25-5 on page 25-13, or enter `snmp-server enable traps ?`            |
|         |                                              | - To enable multiple types of traps, you must enter a separate `snmp-    |
|         |                                              |   server enable traps` command for each trap type.                     |
|         | Note                                         | - When you configure a trap by using the notification type `port-security`, |
|         |                                              |   configure the port security trap first, and then configure the port   |
|         |                                              |   security trap rate:                                                   |
|         |                                              |   - `snmp-server enable traps port-security`                           |
|         |                                              |   - `snmp-server enable traps port-security trap-rate rate`             |
| Step 7  | `snmp-server trap-source interface-id`       | (Optional) Specify the source interface, which provides the IP address   |
|         |                                              |   for the trap message. This command also sets the source IP address    |
|         |                                              |   for informs.                                                         |
| Step 8  | `snmp-server queue-length length`           | (Optional) Establish the message queue length for each trap host. The   |
|         |                                              |   range is 1 to 1000; the default is 10.                               |
| Step 9  | `snmp-server trap-timeout seconds`          | (Optional) Define how often to resend trap messages. The range is 1 to  |
|         |                                              |   1000; the default is 30 seconds.                                      |
| 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.                |
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 CPU Threshold Notification Types and Values

Beginning in privileged EXEC mode, follow these steps to set the CPU threshold notification types and values:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
</tbody>
</table>
| Step 2  | process cpu threshold type \{ total \| process \| interrupt \} rising percentage interval seconds [falling fall-percentage interval seconds] | Set the CPU threshold notification types and values:  
  - `total`—set the notification type to total CPU utilization.  
  - `process`—set the notification type to CPU process utilization.  
  - `interrupt`—set the notification type to CPU interrupt utilization.  
  - `rising percentage`—the percentage (1 to 100) of CPU resources that, when exceeded for the configured interval, sends a CPU threshold notification.  
  - `interval seconds`—the duration of the CPU threshold violation in seconds (5 to 86400) that, when met, sends a CPU threshold notification.  
  - `falling fall-percentage interval seconds`—the percentage (1 to 100) of CPU resources that, when usage falls below this level for the configured interval, sends a CPU threshold notification.  
  
  This value must be equal to or less than the `rising percentage` value. If not specified, the `falling fall-percentage` value is the same as the `rising percentage` value. |
| Step 3  | end | Return to privileged EXEC mode. |
| Step 4  | 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 EXEC command. |
| Step 5  | copy running-config startup-config | (Optional) Save your entries in the configuration file. |
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><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> snmp-server contact <em>text</em></td>
<td>Set the system contact string.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td><code>snmp-server contact Dial System Operator at beeper 21555.</code></td>
</tr>
<tr>
<td><strong>Step 3</strong> snmp-server location <em>text</em></td>
<td>Set the system location string.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td><code>snmp-server location Building 3/Room 222</code></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 running-config</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>

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> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> snmp-server tftp-server-list</td>
<td>Limit TFTP servers used for configuration file copies through SNMP to the servers in the access list.</td>
</tr>
<tr>
<td><code>access-list-number</code></td>
<td>For <code>access-list-number</code>, enter an IP standard access list numbered from 1 to 99 and 1300 to 1999.</td>
</tr>
<tr>
<td><strong>Step 3</strong> access-list <code>access-list-number</code></td>
<td>Create a standard access list, repeating the command as many times as necessary.</td>
</tr>
<tr>
<td><code>deny</code></td>
<td>The <code>deny</code> keyword denies access if the conditions are matched.</td>
</tr>
<tr>
<td><code>permit</code></td>
<td>The <code>permit</code> keyword permits access if the conditions are matched.</td>
</tr>
<tr>
<td><code>source</code> <code>[source-wildcard]</code></td>
<td>For <code>source</code>, enter the IP address of the TFTP servers that can access the switch.</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>
</tbody>
</table>

Recall that the access list is always terminated by an implicit deny statement for everything.
## 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* document 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></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>snmp mib bulkstat object-list <em>list-name</em></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>add {object-name | oid}</td>
</tr>
<tr>
<td></td>
<td>• For <em>object-name</em>, enter the name of the MIB object to add to the list. You can enter only object names from the Interfaces MIB or the Cisco Committed Access Rate MIB.</td>
</tr>
<tr>
<td></td>
<td>• For <em>oid</em>, enter the Object ID of the MIB object to add to the list.</td>
</tr>
<tr>
<td></td>
<td>All the objects in an object-list must be in the same MIB index, but the objects need not belong to the same MIB table. Repeat the command until all objects to be monitored are added.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>snmp mib bulkstat schema <em>schema-name</em></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>object-list <em>list-name</em></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>instance {exact | wild} {interface interface-id | oid oid}</td>
</tr>
<tr>
<td></td>
<td>• Enter <em>exact</em> when the specified instance appended to the object list is the complete OID.</td>
</tr>
<tr>
<td></td>
<td>• Enter <em>wild</em> when all subindices of the specified OID belong to the schema.</td>
</tr>
<tr>
<td></td>
<td>• Enter an <em>interface interface-id</em> to specify an interface ID instead of an instance OID.</td>
</tr>
<tr>
<td></td>
<td>• Enter <em>oid oid</em> to specify an instance OID for the schema.</td>
</tr>
</tbody>
</table>
Chapter 25  Configuring SNMP

Configuring SNMP

This example configures a bulk-statistics object list and schema:

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

Beginning in privileged EXEC mode, follow these steps to configure bulk-statistics transfer options:

<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>snmp mib bulkstat transfer transfer-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>buffer-size bytes</td>
</tr>
<tr>
<td>Step 4</td>
<td>format {bulkBinary</td>
</tr>
<tr>
<td>Step 5</td>
<td>schema schema-name</td>
</tr>
<tr>
<td>Step 6</td>
<td>transfer-interval minutes</td>
</tr>
<tr>
<td>Step 7</td>
<td>url primary URL</td>
</tr>
<tr>
<td>Step 8</td>
<td>retry number</td>
</tr>
<tr>
<td>Step 9</td>
<td>retain minutes</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 schema ASCII
Switch(config-bulk-tr) # buffer-size 2147483647
Switch(config-bulk-tr) # schema testschema1
Switch(config-bulk-tr) # schema testschema2
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

You can use the CLI to configure the Cisco Process MIB CPU threshold table.

**Note**

For commands for configuring the Cisco Process MIB CPU threshold table, see the *Cisco IOS Commands Master List, Release 12.4*, at this URL:


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>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 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>
<tr>
<td></td>
<td>- For <code>entry-percentage number</code>, enter the percentage (1 to 100) of CPU utilization that a process must use to become part of the history table.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) For <code>size seconds</code>, 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.</td>
</tr>
</tbody>
</table>
## 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 MAC notification 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 mac-notification
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 00000063000100a1c0b4011b
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 also can use the other privileged EXEC commands in Table 25-6 to display SNMP information. For information about the fields in the displays, see the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*.

Table 25-6  Commands for Displaying SNMP Information

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show snmp</code></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 been configured on the device.</td>
</tr>
<tr>
<td></td>
<td>remote]`</td>
</tr>
<tr>
<td><code>show snmp group</code></td>
<td>Displays information on each SNMP group on the network.</td>
</tr>
<tr>
<td><code>show snmp mib bulk transfer</code></td>
<td>Displays transfer status of files generated by the Periodic MIB Data Collection and Transfer Mechanism (bulk statistics feature).</td>
</tr>
<tr>
<td><code>show snmp pending</code></td>
<td>Displays information on pending SNMP requests.</td>
</tr>
<tr>
<td><code>show snmp sessions</code></td>
<td>Displays information on the current SNMP sessions.</td>
</tr>
<tr>
<td><code>show snmp user</code></td>
<td>Displays information on each SNMP user name in the SNMP users table.</td>
</tr>
</tbody>
</table>

**Note** You must use this command to display SNMPv3 configuration information for `auth | noauth | priv` mode. This information is not displayed in the `show running-config` output.
Configuring Network Security with ACLs

This chapter describes how to configure network security on the Cisco ME 3800X and 3600X switch by using access control lists (ACLs), which are also referred to in commands and tables as access lists. Information in this chapter about IP ACLs is specific to IP Version 4 (IPv4).

**Note**

ACLs are not supported on ports configured with Ethernet flow point (EFP) service instances.

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 the *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*.

- Understanding ACLs, page 26-1
- Configuring IPv4 ACLs, page 26-6
- Creating Named MAC Extended ACLs, page 26-27
- Configuring VLAN Maps, page 26-30
- Using VLAN Maps with Router ACLs, page 26-36
- Displaying IPv4 ACL Configuration, page 26-40

**Note**

Not all ACL parameters can be used for QoS classification. See the “Ingress Classification Based on QoS ACLs” section on page 27-10.

Understanding ACLs

Packet filtering can help limit network traffic and restrict network use by certain users or devices. ACLs 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. One by one, it tests packets against the conditions in an access list. The first match decides whether the switch accepts or rejects the packets. Because the switch stops testing after the first match, the order of conditions in the list is critical. If no conditions match, the switch rejects the packet. If there are no restrictions, the switch forwards the packet; otherwise, the switch drops the packet. The switch can use ACLs on all packets it forwards.
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 IPv4 ACLs and Ethernet (MAC) ACLs:

- IP ACLs filter IPv4 traffic, including TCP, User Datagram Protocol (UDP), Internet Group Management Protocol (IGMP), and Internet Control Message Protocol (ICMP).
- Ethernet ACLs filter non-IP traffic.

**Note** MAC ACLs are not supported on ports configured with service instances.

This switch also supports quality of service (QoS) classification ACLs. For more information, see the “Understanding QoS” section on page 27-2.

These sections contain this conceptual information:

- Supported ACLs, page 26-2
- Handling Fragmented and Unfragmented Traffic, page 26-5

### Supported ACLs

The switch supports three applications of ACLs to filter traffic:

- 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.

  **Note** Port ACLs are not supported on ports configured with service instances.

- Router ACLs access-control routed traffic between VLANs and are applied to Layer 3 interfaces in a specific direction (inbound or outbound). The switch must be running the metro IP access image to support router ACLs.

- VLAN ACLs or VLAN maps access-control all packets (forwarded 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 IPv4. Unsupported protocols are access-controlled through MAC addresses using Ethernet ACEs. After a VLAN map is applied to a VLAN, all packets 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 input port ACLs, router 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 IPv4 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 IPv4 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 IPv4 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 IPv4 packets are filtered by both the VLAN map and the router ACL. Other packets are filtered only by the VLAN map.

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 and you can apply them only in the inbound direction. You cannot apply an ACL to a port configured with a service instance.

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

The switch examines ACLs associated with all inbound features configured on a given interface and permits or denies packet forwarding based on how the packet matches the entries in the ACL. In this way, ACLs are used to control access to a network or to part of a network. Figure 26-1 is an example of using port ACLs to control access to a network when all workstations are 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. Port ACLs can only be applied to Layer 2 interfaces in the inbound direction.
Understanding ACLs

Figure 26-1  Using ACLs to Control Traffic to a Network

When you apply a port ACL to a trunk port, the ACL filters traffic on all VLANs present on the trunk port. You cannot apply a port ACL to a port configured with a service instance.

With port ACLs, you can filter IP traffic by using IP access lists and non-IP 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.

Router ACLs

You can apply router ACLs on switch virtual interfaces (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.

The switch supports these access lists for IPv4 traffic:

- 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.
As with port ACLs, the switch examines ACLs associated with features configured on a given interface. However, router ACLs are supported in both directions. 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 26-1, ACLs applied at the router input allow Host A to access the Human Resources network, but prevent Host B from accessing the same network.

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 forwarded within a VLAN in the switch. VLAN maps are used for security packet filtering and are not defined by direction (input or output).

You can configure VLAN maps to match Layer 3 addresses for IPv4 traffic. All non-IP 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 26-2 shows how a VLAN map is applied to prevent a specific type of traffic from Host A in VLAN 10 from being forwarded. You can apply only one VLAN map to a VLAN. The map is applied to all switchports in the VLAN, including ports configured with service instances with a bridge domain equal to the VLAN.

Handling Fragmented and Unfragmented Traffic

IPv4 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.
Chapter 26
Configuring Network Security with ACLs

Configuring IPv4 ACLs

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 IPv4 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

Note
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.
- 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 IPv4 ACLs

Configuring IPv4 ACLs on the switch is the same as configuring IPv4 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 the *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*.

The switch does not support these Cisco IOS router ACL-related features:

- Non-IP protocol ACLs (see Table 26-1 on page 26-8) or bridge-group ACLs
• IP accounting
• Inbound and outbound rate limiting (except with QoS ACLs)
• Reflexive ACLs or dynamic ACLs
• 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 the access conditions.
**Step 2**  Apply the ACL to interfaces or terminal lines. You can also apply standard and extended IP ACLs to VLAN maps.

These sections contain this configuration information:

• Creating Standard and Extended IPv4 ACLs, page 26-7
• Applying an IPv4 ACL to a Terminal Line, page 26-18
• Applying an IPv4 ACL to an Interface, page 26-19
• Hardware and Software Treatment of IP ACLs, page 26-20
• Troubleshooting ACLs, page 26-21
• IPv4 ACL Configuration Examples, page 26-22

### Creating Standard and Extended IPv4 ACLs

This section describes IP ACLs. An ACL is a sequential collection of permit and deny conditions. One by one, the switch tests packets against the conditions in an access list. The first match determines whether the switch accepts or rejects the packet. Because the switch stops testing 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 IPv4:

• 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:

• IPv4 Access List Numbers, page 26-8
• ACL Logging, page 26-8
• Creating a Numbered Standard ACL, page 26-9
• Creating a Numbered Extended ACL, page 26-10
• Resequencing ACEs in an ACL, page 26-14
• Creating Named Standard and Extended ACLs, page 26-14
• Using Time Ranges with ACLs, page 26-16
• Including Comments in ACLs, page 26-18
IPv4 Access List Numbers

The number you use to denote your IPv4 ACL shows the type of access list that you are creating. Table 26-1 lists the access-list number and corresponding access list type and shows whether or not they are supported in the switch. The switch supports IPv4 standard and 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>
<tr>
<td>1300–1999</td>
<td>IP standard access list (expanded range)</td>
<td>Yes</td>
</tr>
<tr>
<td>2000–2699</td>
<td>IP extended access list (expanded range)</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Note

In addition to numbered standard and extended IPv4 ACLs, you can also create standard and extended named IPv4 ACLs by using the supported 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.

ACL Logging

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.

Note

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.
Creating a Numbered Standard ACL

Beginning in privileged EXEC mode, follow these steps to create a numbered standard ACL:

Step 1: configure terminal

Enter global configuration mode.

Step 2: access-list access-list-number [deny | permit] source [source-wildcard] [log]

Define a standard IPv4 access list 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 from which the packet is being sent specified as:

- The 32-bit quantity in dotted-decimal format.
- 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.
- The keyword host as an abbreviation for source and source-wildcard of source 0.0.0.0.

(Optional) The source-wildcard applies wildcard bits to the source.

(Optional) Enter log to cause an informational logging message about the packet that matches the entry to be sent to the console.

Step 3: end

Return to privileged EXEC mode.

Step 4: show access-lists [number | name]

Show the access list configuration.

Step 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 ACL. You cannot delete individual ACEs from numbered access lists.

Note: 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.

```bash
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.

After creating a numbered standard IPv4 ACL, you can apply it to terminal lines (see the “Applying an IPv4 ACL to a Terminal Line” section on page 26-18), to interfaces (see the “Applying an IPv4 ACL to an Interface” section on page 26-19), or to VLANs (see the “Configuring VLAN Maps” section on page 26-30).

### 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)
- 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)
- 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 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.

If you are creating ACLs to be used for quality of service (QoS) classification, these limitations apply:
- QoS ACLs support only the permit action.
- For permit protocol, the supported keywords are: gre, icmp, igmp, ipinip, tcp, and udp.
For source and destination address, the supported entries are ip-address, any, or host.

See the “Using ACLs to Classify Traffic” section on page 27-35.

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></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2a</td>
<td></td>
</tr>
</tbody>
</table>
| access-list access-list-number {deny | permit} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp] | Define an extended IPv4 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 26-16. • 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. 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.
**Chapter 26      Configuring Network Security with ACLs**

**Configuring IPv4 ACLs**

or

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list access-list-number</td>
<td>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.</td>
</tr>
<tr>
<td>{deny</td>
<td>permit} protocol any any [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp]</td>
</tr>
<tr>
<td>or access-list access-list-number</td>
<td>Define an extended IP access list by using an abbreviation for a source and a destination 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 the source and destination wildcard or mask.</td>
</tr>
<tr>
<td>{deny</td>
<td>permit} protocol host source host destination [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp]</td>
</tr>
<tr>
<td>Step 2b access-list access-list-number</td>
<td>(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 other 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).</td>
</tr>
<tr>
<td>Step 2c access-list access-list-number</td>
<td>(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 the [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.</td>
</tr>
</tbody>
</table>
### Configuring IPv4 ACLs

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 to 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.

<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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Optional) Define an extended ICMP access list and the access conditions. Enter <code>icmp</code> 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:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <code>icmp-type</code>—Enter to filter by ICMP message type, a number from 0 to 255.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <code>icmp-code</code>—Enter to filter ICMP packets that are filtered by the ICMP message code type, a number from 0 to 255.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <code>icmp-message</code>—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 <code>?</code>, or see the “Configuring IP Services” section of the <code>Cisco IOS IP Configuration Guide, Release 12.2</code>.</td>
</tr>
<tr>
<td>2e</td>
<td>`access-list access-list-number deny</td>
<td>permit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Optional) Define an extended IGMP access list and the access conditions. Enter <code>igmp</code> for Internet Group Management Protocol. The IGMP parameters are the same as those described for most IP protocols in Step 2a, with this optional parameter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <code>igmp-type</code>—To match IGMP message type, enter a number from 0 to 15, or enter the message name (<code>host-query</code>, <code>host-report</code>, <code>pim</code>, or <code>trace</code>).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Note</em> Although visible in the command-line help, <code>dvmrp</code> is not supported.</td>
</tr>
<tr>
<td>3</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>4</td>
<td>`show access-lists [number</td>
<td>name]`</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>
After creating a numbered extended ACL, you can apply it to terminal lines (see the “Applying an IPv4 ACL to a Terminal Line” section on page 26-18), to interfaces (see the “Applying an IPv4 ACL to an Interface” section on page 26-19), or to VLANs (see the “Configuring VLAN Maps” section on page 26-30).

Resequencing ACEs in an ACL

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 IPv4 ACLs with an alphanumeric string (a name) rather than a number. You can use named ACLs to configure more IPv4 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.

Note
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 IPv4 ACLs” section on page 26-7.
- 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><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>ip access-list standard name</code></td>
<td>Define a standard IPv4 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.
## Configuring IPv4 ACLs

### 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>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 access-list extended name</td>
</tr>
<tr>
<td>Note</td>
<td>The name can be a number from 100 to 199.</td>
</tr>
<tr>
<td>Step 3</td>
<td>deny</td>
</tr>
<tr>
<td></td>
<td>{ source [source-wildcard]</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>permit</td>
</tr>
<tr>
<td></td>
<td>{ source [source-wildcard]</td>
</tr>
<tr>
<td></td>
<td>protocol</td>
</tr>
<tr>
<td></td>
<td>{ source [source-wildcard]</td>
</tr>
</tbody>
</table>

### 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.
Chapter 26  Configuring Network Security with ACLs

This example shows how you can delete individual ACEs from the named access list border-list:

```plaintext
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 IPv4 ACL to an Interface” section on page 26-19) or to VLANs (see the “Configuring VLAN Maps” section on page 26-30).

### 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 IPv4 ACLs” section on page 26-7, and the “Creating Named Standard and Extended ACLs” section on page 26-14.

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 effect 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 a time-range parameter for an 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>time-range time-range-name</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 26 Configuring Network Security with ACLs

### Configuring IPv4 ACLs

Repeat the steps if you want multiple items 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 to configure January 1, 2006 as a company 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_2006
Switch(config-time-range)# absolute start 00:00 1 Jan 2006 end 23:59 1 Jan 2006
Switch(config-time-range)# exit
Switch(config)# show time-range
```  

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_2006
Switch(config)# access-list 188 permit tcp any any time-range workhours
Switch(config)# end
Switch(config)# show access-lists
Extended IP access list 188
  10 deny tcp any any time-range new_year_day_2006 (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_2006
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(config)# show ip access-lists
Extended IP access list deny_access
  10 deny tcp any any time-range new_year_day_2006 (inactive)
Extended IP access list may_access
  10 permit tcp any any time-range workhours (inactive)
```

### Command and Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</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. |
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` command. To remove the remark, use the `no` form of this command.

In this example, the workstation that belongs to Jones is allowed access, and the workstation that belongs 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 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 IPv4 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 IPv4 ACL to an Interface” section on page 26-19. For applying ACLs to VLANs, see the “Configuring VLAN Maps” section on page 26-30.

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 <code>line-number</code> 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>
</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 IPv4 ACL to an Interface

This section describes how to apply IPv4 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:

- You cannot apply an ACL to a port configured with a service instance. Layer 2 ACLs are not supported on these ports.
- 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
When you apply an egress ACL to an interface all local traffic is blocked, even when `ip access-list match-local-traffic` command is not configured.

#### 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><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>interface interface-id</code></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>
</tbody>
</table>
Configuring IPv4 ACLs

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 to a port to filter packets entering the port:

```
Switch(config)# interface gigabitethernet0/1
Router(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.

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.
Chapter 26  Configuring Network Security with ACLs

Configuring IPv4 ACLs

Note

If an ACL configuration cannot be implemented in hardware due to an out-of-resource condition on a switch, then only the traffic in that VLAN arriving on that switch is affected (forwarded in software). Software forwarding of packets might adversely impact the performance of the switch, depending on the number of CPU cycles that this consumes.

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. 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:

```plaintext
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
```

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:
  ```plaintext
  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.

## IPv4 ACL Configuration Examples

This section provides examples of configuring and applying IPv4 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 26-3** shows a small networked office environment with 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.
Figure 26-3 Using Router ACLs to Control Traffic

Server A
Benefits

Server B
Payroll

Port 2 Port 1

Human Resources
172.20.128.0-31

Accounting
172.20.128.64-95

Benefits

Payroll
This example uses a standard ACL to filter traffic coming into Server B from a port, 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 gigabitethernet0/1
Switch(config-if)# ip access-group 6 out
```

This example uses an extended ACL to filter traffic coming from Server B into a port, 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 gigabitethernet0/1
Switch(config-if)# ip access-group 106 in
```

### 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 applied to packets entering a port.

```
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
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 2 in
```

### 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
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 102 in
```

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. Gigabit Ethernet interface 1 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
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 102 in
```

**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.

```
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 `Internet_filter` ACL is applied to outgoing traffic and the `marketing_group` ACL is applied to incoming traffic on a Layer 3 port.

```
Switch(config)# interface gigabitethernet0/2
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).

```
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
```
Chapter 26      Configuring Network Security with ACLs

Configuring IPv4 ACLs

!  
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 gigabitethernet0/1  
Switch(config-if)# ip access-group strict in

Commented IP ACL Entries

In this example of a numbered ACL, the workstation that belongs to Jones is allowed access, and the workstation that belongs 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

In this example of a numbered ACL, the Winter and Smith workstations are not allowed to browse the web:

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 gigabitethernet0/1  
Switch(config-if)# ip access-group stan1 in  
Switch(config-if)# end  
Switch# show logging

Syslog 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
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 or to Layer 2 interfaces configured with service instances.

For more information about the supported non-IP protocols in the `mac access-list extended` command, see the command reference for this release.
**Creating Named MAC Extended ACLs**

**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>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>mac access-list extended name</code></td>
</tr>
</tbody>
</table>
| Step 3  | `{deny | permit} {any | host source MAC address | source MAC address mask} {any | host destination MAC address | destination MAC address mask} {type mask | lsap lsap mask | aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp | 0-65535} [cos cos]` | In extended MAC access-list configuration mode, specify to `permit` or `deny` any source MAC address, a source MAC address with a mask, or a specific `host` source MAC address and any destination MAC address, destination MAC address with a mask, or a specific destination MAC address. (Optional) You can also enter these options:
  - `type mask`—An arbitrary EtherType number of a packet with Ethernet II or SNAP encapsulation in decimal, hexadecimal, or octal with optional mask of `don’t care` bits applied to the EtherType before testing for a match.
  - `lsap lsap mask`—An LSAP number of a packet with IEEE 802.2 encapsulation in decimal, hexadecimal, or octal with optional mask of `don’t care` bits.
  - `cos cos`—An IEEE 802.1Q cost of service number from 0 to 7 used to set priority. |
| Step 4  | `end` | Return to privileged EXEC mode. |
| Step 5  | `show access-lists [number | name]` | Show the access list configuration. |
| Step 6  | `copy running-config startup-config` | (Optional) Save your entries in the configuration file. |

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
Switch(config-ext-macl)# end
Switch# show access-lists
Extended MAC access list mac1
  10 deny   any any decnet-iv
  20 permit any
```
Chapter 26 Configuring Network Security with ACLs

Creating Named MAC Extended ACLs

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-IP traffic coming in that interface. When you apply the MAC ACL, consider these guidelines:

- You cannot apply named MAC extended ACLs to Layer 3 interfaces or to Layer 2 interfaces configured with service instances.
- 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 IP packets, and the MAC access list filters non-IP 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>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>mac access-group {name} {in}</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show mac access-group [interface interface-id]</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</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 to a port to filter packets entering the port:

```
Switch(config)# interface gigabitethernet0/2
Router(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 IPv4 ACLs or named MAC extended ACLs that you want to apply to the VLAN. See the “Creating Standard and Extended IPv4 ACLs” section on page 26-7 and the “Creating a VLAN Map” section on page 26-31.

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 IP packet or a non-IP 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 has 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.

These sections contain this configuration information:
- VLAN Map Configuration Guidelines, page 26-30
- Creating a VLAN Map, page 26-31
- Applying a VLAN Map to a VLAN, page 26-34
- Using VLAN Maps in Your Network, page 26-34

VLAN Map Configuration Guidelines

- 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.
Chapter 26      Configuring Network Security with ACLs

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>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>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>action {drop</td>
<td>forward}</td>
</tr>
<tr>
<td>match {ip</td>
<td>mac} address {name</td>
</tr>
<tr>
<td>end</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Display the access list configuration.</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 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.

```plaintext
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.

```plaintext
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-IP packets

```plaintext
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
```
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-IP packets
- Forward all IP packets

```bash
Switch(config)# mac access-list extended good-hosts
Switch(config-ext-macl)# permit host 000.0c00.0111 any
Switch(config-ext-macl)# permit host 000.0c00.0211 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 (IP and non-IP). 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

```bash
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</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>vlan filter mapname vlan-list list</td>
</tr>
<tr>
<td>Step 3</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 4</td>
<td>copy running-config startup-config</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

- Wiring Closet Configuration, page 26-34
- Denying Access to a Server on Another VLAN, page 26-35

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 26-4, 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, a Layer 3 switch with routing enabled. Traffic from Host X to Host Y can be access-controlled at the traffic entry point, Switch A.
Figure 26-4  Wiring Closet Configuration

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) at Switch A and not forward it to Switch B.

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 26-5):

- 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 SERVER 1 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 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. If a packet flow matches a VLAN-map deny clause in the ACL, regardless of the router ACL configuration, the packet flow is denied.

---

**Note**

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.

These sections contain information about using VLAN maps with router ACLs:

- VLAN Maps and Router ACL Configuration Guidelines, page 26-37
- Examples of Router ACLs and VLAN Maps Applied to VLANs, page 26-38

**VLAN Maps and Router ACL Configuration Guidelines**

These guidelines are for configurations where you need to have an 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, 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 26-6 shows how an ACL is applied on packets that are switched within a VLAN. Packets switched within the VLAN without being routed or forwarded are only subject to the VLAN map of the input VLAN.

**Figure 26-6 Applying ACLs on Switched Packets**

ACLs and Routed Packets

Figure 26-7 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 26-8 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 26-8) drops the packet, no destination receives a copy of the packet.
Displaying IPv4 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 26-2 to display this information.

### Table 26-2 Commands for Displaying Access Lists and Access Groups

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show access-lists [number \ name]</code></td>
<td>Displays 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 [number \ name]</code></td>
<td>Displays the contents of all current IP access lists or a specific IP access list (numbered or named).</td>
</tr>
<tr>
<td><code>show ip interface interface-id</code></td>
<td>Displays 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><code>show running-config [interface interface-id]</code></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><code>show mac access-group [interface interface-id]</code></td>
<td>Displays MAC access lists applied to all Layer 2 interfaces or the specified Layer 2 interface.</td>
</tr>
</tbody>
</table>

You can also display information about VLAN access maps or VLAN filters. Use the privileged EXEC commands in Table 26-3 to display VLAN map information.

### Table 26-3 Commands for Displaying VLAN Map Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show vlan access-map [mapname]</code></td>
<td>Shows 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>
CHAPTER 27

Configuring Quality of Service (QoS)

This chapter describes how to configure quality of service (QoS) on the ME 3800X and ME 3600X switches by using the modular QoS command-line interface (MQC) commands. With QoS, you can provide preferential treatment to certain types of traffic at the expense of other types. When you do not configure QoS, the switch offers best-effort service to each packet, regardless of the packet contents or size. MQC provides a hierarchical configuration framework for prioritizing or limiting specific streams of traffic.

QoS includes traffic classification, marking, policing, queuing, and scheduling configured with service policies that are attached to ingress and egress targets. On the ME 3800X and ME 3600X switches, targets can be switchports or Ethernet Flow Points (EFPs), also referred to as service instances. The switches do not support the service policies attached to the EtherChannel port channels although you can attach them to ports that belong to an EtherChannel as long as there are no EFPs configured on the EtherChannel.

Ingress QoS includes classification, marking, and policing. Classification can be based on the class of service (CoS), Differentiated Services Code Point (DSCP), IP precedence, or the multiprotocol label switching (MPLS) experimental (EXP) value in the inbound packet. You can classify based on Layer 2 MAC, IP-standard, or IP-extended access control lists (ACLs).

Egress QoS supports the same classifications as ingress QoS except for ACLs, and also includes classification based on QoS group or discard class. Egress QoS also includes queueing based on the weighted tail drop (WTD) algorithm, scheduling based on shaped weights, and an egress priority queue.

You can also use hierarchical QoS to classify, police, mark, queue, and schedule inbound or outbound traffic. You can define a policy map for the first, second, or third level of the hierarchy. Hierarchical QoS offers classification based on the CoS, DSCP, IP precedence, or the MPLS EXP bits in the packet, and classifying a packet based on its VLAN. The switch supports two-rate, three-color policing at different levels. Drop policy actions include passing the packet through without modification is supported and ingress and egress however, marking down the CoS, DSCP, IP precedence, or the MPLS EXP bits in the packet; or dropping the packet is only supported at ingress.

- Understanding QoS, page 27-2
- Configuring QoS, page 27-30
- Displaying QoS Information, page 27-72

For more information about Cisco IOS MQC commands, see the “Cisco IOS Quality of Service Solutions Command Reference:”


For complete syntax and usage information for the platform-specific commands used in this chapter, see the command reference for this release.
Understanding QoS

When networks operate on a best-effort delivery basis, all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped. When you configure QoS, you can select specific network traffic, prioritize it according to its relative importance, and use traffic-management techniques to provide preferential treatment. Implementing QoS in your network makes network performance more predictable and bandwidth utilization more effective.

Figure 27-1 shows the MQC model.

![Figure 27-1 Modular QoS CLI Model](image)

Basic QoS includes these actions.

- Packet classification organizes traffic on the basis of whether or not the traffic matches a specific criteria. When a packet is received, the switch identifies all key packet fields: CoS, DSCP, IP precedence, or MPLS EXP. The switch classifies the packet based on this content or based on an ACL lookup. The class `class-default` is used in a policy map for any traffic that does not explicitly match any other class in the policy map. See the “Classification” section on page 27-5.

- Packet policing determines whether a packet is in or out of profile by comparing the rate of the incoming traffic to the configured policer. You can configure a committed information rate (CIR) and peak information rate (PIR) and set actions to perform on packets that conform to the CIR and PIR (conform-action), packets that conform to the PIR, but not the CIR (exceed-action), and packets that exceed the PIR value (violate-action). See the “Policing” section on page 27-15.

- All packets that belong to a classification can be remarked. When you configure a policer, packets that meet or exceed the permitted bandwidth requirements (bits per second) can be conditionally passed through, dropped, or marked. You use the `police` command to conditionally mark incoming packets based on the CIR and PIR. You use the `set` command to unconditionally mark packets. See the “Packet Marking” section on page 27-18.

- Congestion management uses queuing and scheduling algorithms to queue and sort traffic that is leaving a port. The switch supports these scheduling and traffic-limiting features: class-based weighted fair queuing (CBWFQ), class-based traffic shaping, port shaping, and class-based priority queuing. You can provide guaranteed bandwidth to a particular class of traffic while still servicing other traffic queues. See the “Congestion Management and Scheduling” section on page 27-23.

- Queuing on the switch uses the WTD algorithm, a congestion-avoidance mechanism. WTD differentiates traffic classes and regulates the queue size based on the classification. See the “Congestion Avoidance and Queuing” section on page 27-19.

This section includes information about these topics:

- Modular QoS CLI Configuration, page 27-3
Modular QoS CLI Configuration

With the modular QoS CLI, you create traffic policies and attach these policies to physical interfaces or EFP service instances. A traffic policy contains a traffic class and one or more QoS features. You define a traffic class to classify traffic, use a traffic policy to define how to treat the classified traffic, and attach the policy to a port or service instance to create a service policy.

---

**Step 1** Define a traffic class.

Use the `class-map` global configuration command to define a traffic flow or class and to enter class-map configuration mode. A traffic class contains:

- A name—You name the traffic class in the `class-map` command line to enter class-map configuration mode.
- (Optional) Keywords to evaluate the match commands, either `class-map match-any` or `class-map match-all`. By default, match-all is supported with a class map is defined and match-any is not specified. Only one match statement is allowed for match-all, except for outer VLAN and inner VLAN, or outer CoS and inner CoS matches for 802.1Q tunneling (QinQ) packets.
- A series of `match` class-map configuration commands to specify criteria for classifying packets. Criteria can include matching an access group defined by an ACL or matching a specific list of COS, DSCP, IP precedence, or MPLS EXP values. If a packet matches the specified criteria, that packet is considered a member of the class and is forwarded according to the QoS specifications set in the traffic policy. Packets that do not meet any of the matching criteria are classified as members of the default traffic class.

**Note** For exceptions to the list of match statements, see the “Classification” section on page 27-5.

**Step 2** Associate policies and actions with each traffic class.

Use the `policy-map` global configuration command to create a traffic policy and to enter policy-map configuration mode. A traffic policy specifies the traffic class to act on and defines the QoS features to associate with the specified traffic class. A traffic policy contains a name, a traffic class (specified with the `class` policy-map configuration command), and the QoS policies configured in the class.

- A name—You name the traffic policy in the `policy-map` command line to enter policy-map configuration mode.
- A traffic class—Use the `class` policy-map configuration command to enter the name of the traffic class used to classify traffic to the specified policy, and enter policy-map class configuration mode.
• The QoS features to apply to the classified traffic. These include the `set` or `police` commands for input policy maps or the `bandwidth`, `priority`, `queue-limit` or `shape average` commands for output policy maps.

**Note**
A packet can match only one traffic class within a traffic policy. If a packet matches more than one traffic class in the traffic policy, the first traffic class defined in the policy is used. To configure more than one match criterion for packets, you can associate multiple traffic classes with a single traffic policy.

**Step 3**
Attach the traffic policy to a target, which can be an interface or an EFP service instance.

Use the `service-policy` interface configuration command to attach the policy map to a target and to specify if the policy should be applied to packets that enter or leave the target. For example, entering the `service-policy output policy1` interface configuration command attaches all the characteristics of the traffic policy named `class1` to the interface. Entering the `service-policy output policy1` service instance configuration command attaches all the characteristics of the traffic policy named `class1` to the EFP service policy. All packets leaving the target are evaluated according to the criteria specified in the traffic policy `class1`.

**Note**
If you enter the `no policy-map policy-map-name` global configuration command to delete a policy map that is attached to an interface or service instance, a warning message appears that lists any interfaces from which the policy map is being detached. The policy map is then detached and deleted. For example:

```
Warning: Detaching Policy test1 from Interface GigabitEthernet0/1
```

**Hierarchical QoS**

Hierarchical QoS configuration involves traffic classification, policing, queuing, 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 a port or EFP. You can omit hierarchical levels, but the order of levels (class level, VLAN level, and then physical level) must be preserved.

You can configure three QoS levels in the hierarchy:

• Class level—You configure this level of the hierarchy by matching CoS, DSCP, IP precedence, MAC ACLs, IP ACLs, QoS groups, discard-class, or MPLS EXP bits in the packet by using the `match` commands.

```
match access-group name | cos [inner] cos-list | discard-class value | dscp dscp-list | ip precedence ip-precedence-list | mpls experimental exp-list | qos-group value
```

At the class level, you can use policy-map class configuration commands to:

- Configure policer drops by using the `police cir` or `police cir percent` command.
- Configure tail drop policies by using the `queue-limit` command.
- Modify the traffic class by setting Layer 2 and Layer 3 QoS fields by using the `set` commands.
- Configure scheduling by using the `bandwidth` or the `priority` command.
- Configure traffic shaping by using the `shape` command.

• VLAN level—You configure per-VLAN QoS by entering the match `vlan vlan-id` or `match vlan-inner vlan-id` class-map configuration command for one or more VLANs.
At the VLAN level, you can:

- Configure the VLANs to police ingress traffic by using the `police cir` or `police cir percent` policy command.
- Configure unconditional marking on ingress traffic by using the `set` command.
- Configure the queue to share the available port bandwidth and enable CBWFQ by using the `bandwidth` command.
- Configure traffic shaping by using the `shape` command.

You can also 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 to apply the class-level policy only to traffic that matches the VLAN class. You cannot mix VLAN-level and class-level matches within a class map.

- 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 that does match the parent policy. If no parent policy is configured, the parent policy represents the physical port.
  - Configure unconditional marking by using the `set` command.
  - 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 a physical port or to an EFP.

**Classification**

Classification distinguishes one kind of traffic from another by examining the fields in the packet header. When a packet is received, the switch examines the header and identifies all key packet fields. A packet can be classified based on an ACL, on the DSCP, the CoS, IP precedence, or MPLS EXP value in the packet, or by the VLAN ID. Figure 27-2 has examples of classification information carried in a Layer 2 or a Layer 3 IP packet header, using six bits from the deprecated IP type of service (ToS) field to carry the classification information.

- Layer 2 frame headers have a 2-byte Tag Control Information field that carries the CoS value, called the User Priority bits, in the 3 most-significant bits, and the VLAN ID value in the 12 least-significant bits. Layer 2 CoS values range from 0 to 7.
- 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. MPLS EXP values range from 0 to 7.
The match Command

In class-map configuration mode, you use the **match** class-map configuration command to define the match criterion for the traffic. You can also create a class map that requires that all matching criteria in the class map be in the packet header by using the **class map match-all** class-map name global configuration command.
Chapter 27  Configuring Quality of Service (QoS)

Understanding QoS

The **match-all** keyword is supported only for outer and inner VLAN, or outer and inner CoS matches for QinQ packets and is rejected for all other mutually exclusive match criteria. You can configure only one match entry in a **match-all** class map.

You can use the **class map match-any class-map name** global configuration command to define a classification with any of the listed criteria.

In class-map configuration mode, you use the **match** command to specify the classification criteria. If a packet matches the configured criteria, it belongs to a specific class and is forwarded according to the specified policy. For example, you can use the **match class-map command with CoS, IP DSCP, IP precedence, or MPLS EXP values. You can also match an access group, a QoS group, or a VLAN ID or inner VLAN ID or VLAN ID range for per-port, per-VLAN QoS.

For an input policy map, you cannot configure both an IP classification (match ip dscp, **match ip precedence, match ip acl**) and a non-IP classification (**match mac acl**) in the same policy map or class map.

This example shows how to create a class map **example** to define a class that matches any of the listed criteria. In this example, if a packet is received with the DSCP equal to 32 or a 40, the packet is identified (classified) by the class map.

```plaintext
Switch(config)# class-map match-any example
Switch(config-cmap)# match ip dscp 32
Switch(config-cmap)# match ip dscp 40
Switch(config-cmap)# exit
```

**VLAN Match Support**

The VLAN Match support feature allows classification based on VLAN on the main interface, which has EVC service instances configured on that interface.

Support VLAN-based policy on an EVC physical-port with the following EFP configuration:

- EFP VLAN encapsulation = Bridge-domain ID
- EFP rewrite = pop-1 ingress symmetric
- VLAN match in the class-map must be same as the Bridge-domain ID

**Restrictions and Guidelines**

The following restrictions apply to VLAN match support:

- The feature is only supported on main interfaces where the EVC Bridge Domain is configured.
- VLAN classification based policy-map, applied on the main interface where QoS on EVC is also configured, is not supported.
- We recommend you not use this feature with huge scale EVC configuration on the main interface as you may run out TCAMS.
- The VLAN match feature is supported on egress only.

The following example shows classification based on VLAN on the main interface, where an EVC is configured.

```plaintext
Switch(config)# class-map match-any vlan_class
Switch(config-cmap)# match vlan 200
Switch(config-cmap)# policy-map main-interface-policy
Switch(config-pmap)# class vlan_class
```
Classification Based on Layer 2 CoS

You use the `match cos` command to classify Layer 2 traffic based on the CoS value, which ranges from 0 to 7.

This example shows how to create a class map to match a CoS value of 5:

```
Switch(config)# class-map premium
Switch(config-cmap)# match cos 5
Switch(config-cmap)# exit
```

Classification Based on IP Precedence

You can classify IPv4 traffic based on the packet IP precedence values, which range from 0 to 7. This example shows how to create a class map to match an IP precedence value of 4:

```
Switch(config)# class-map sample
Switch(config-cmap)# match ip precedence 4
Switch(config-cmap)# exit
```

Classification Based on IP DSCP

When you classify IPv4 traffic based on the IP DSCP value and enter the `match ip dscp` class-map configuration command, you have several classification options:

- Entering a specific DSCP value (0 to 63).
- Using the Default service, which corresponds to an IP precedence and DSCP value of 0. The default per-hop behavior (PHB) is usually best-effort service.
- Using Assured Forwarding (AF) by entering the binary representation of the DSCP value. AF sets the relative probability that a specific class of packets is forwarded when congestion occurs and the traffic does not exceed the maximum permitted rate. AF per-hop behavior delivers IP packets in four different AF classes: AF11-13 (the highest), AF21-23, AF31-33, and AF41-43 (the lowest). Each AF class could be allocated a specific amount of buffer space and drop probabilities, specified by the binary form of the DSCP number. When congestion occurs, the drop precedence of a packet determines the relative importance of the packet within the class. An AF41 class provides the highest probability of a packet being forwarded from one end of the network to the other.
- Entering Class Selector (CS) service values of 1 to 7, corresponding to IP precedence bits in the ToS field of the packet.
- Using Expedited Forwarding (EF) to specify a low-latency path. This corresponds to a DSCP value of 46. EF services use priority queuing to preempt lower priority traffic classes.

This display shows the available classification options:

```
Switch(config-cmap)# match ip dscp ?
<0-63>     Differentiated services codepoint value
af11       Match packets with AF11 dscp (001010)
```
Chapter 27 Configuring Quality of Service (QoS)

Understanding QoS

<table>
<thead>
<tr>
<th>AF</th>
<th>DSCP Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>af12</td>
<td>001100</td>
<td>Match packets with AF12 dscp (001100)</td>
</tr>
<tr>
<td>af13</td>
<td>001110</td>
<td>Match packets with AF13 dscp (001110)</td>
</tr>
<tr>
<td>af21</td>
<td>010010</td>
<td>Match packets with AF21 dscp (010010)</td>
</tr>
<tr>
<td>af22</td>
<td>010100</td>
<td>Match packets with AF22 dscp (010100)</td>
</tr>
<tr>
<td>af23</td>
<td>010110</td>
<td>Match packets with AF23 dscp (010110)</td>
</tr>
<tr>
<td>af31</td>
<td>011010</td>
<td>Match packets with AF31 dscp (011010)</td>
</tr>
<tr>
<td>af32</td>
<td>011100</td>
<td>Match packets with AF32 dscp (011100)</td>
</tr>
<tr>
<td>af33</td>
<td>011110</td>
<td>Match packets with AF33 dscp (011110)</td>
</tr>
<tr>
<td>af41</td>
<td>100010</td>
<td>Match packets with AF41 dscp (100010)</td>
</tr>
<tr>
<td>af42</td>
<td>100100</td>
<td>Match packets with AF42 dscp (100100)</td>
</tr>
<tr>
<td>af43</td>
<td>100110</td>
<td>Match packets with AF43 dscp (100110)</td>
</tr>
<tr>
<td>CS1</td>
<td>001000</td>
<td>Match packets with CS1 (precedence 1) dscp (001000)</td>
</tr>
<tr>
<td>CS2</td>
<td>010000</td>
<td>Match packets with CS2 (precedence 2) dscp (010000)</td>
</tr>
<tr>
<td>CS3</td>
<td>011000</td>
<td>Match packets with CS3 (precedence 3) dscp (011000)</td>
</tr>
<tr>
<td>CS4</td>
<td>100000</td>
<td>Match packets with CS4 (precedence 4) dscp (100000)</td>
</tr>
<tr>
<td>CS5</td>
<td>101000</td>
<td>Match packets with CS5 (precedence 5) dscp (101000)</td>
</tr>
<tr>
<td>CS6</td>
<td>110000</td>
<td>Match packets with CS6 (precedence 6) dscp (110000)</td>
</tr>
<tr>
<td>CS7</td>
<td>111000</td>
<td>Match packets with CS7 (precedence 7) dscp (111000)</td>
</tr>
<tr>
<td>Default</td>
<td>000000</td>
<td>Match packets with default dscp (000000)</td>
</tr>
<tr>
<td>EF</td>
<td>101110</td>
<td>Match packets with EF dscp (101110)</td>
</tr>
</tbody>
</table>

For more information on DSCP prioritization, see RFC-2597 (AF per-hop behavior), RFC-2598 (EF), or RFC-2475 (DSCP).

CoS Mapping

The switch uses EVC and EFPs to support VLAN mapping from the customer VLAN-ID (C-VLAN) to a service-provider VLAN-ID (S-VLAN). See the “Configuring IEEE 802.1Q Tunneling and Layer 2 Protocol Tunneling Using EFPs” section on page 12-18.

For QoS, you can set the service-provider CoS (S-CoS) from either the customer CoS (C-CoS) or the customer DSCP (C-DSCP) value. You can map the inner CoS to the outer CoS for any traffic with traditional 802.1Q tunneling (QinQ). This allows copying the customer CoS into the service provider network.

By default, the switch supports C-CoS to S-CoS propagation for QinQ. When you configure QinQ, you can also set the S-CoS from C-DSCP.

Configuring CoS matching on EFPs configured for tunneling:

- On service instances configured for 802.1Q tunneling, the CoS value of the VLAN tag (inner VLAN or C-VLAN) received on the interface (C-CoS) is automatically reflected in the tunnel VLAN tag (outer VLAN or S-VLAN) by default.

- The set cos policy-map class configuration commands always apply to the outer-most VLAN tag after processing is complete, that is the S-VLAN-ID. For example, in 802.1Q tunnels, entering a set cos command changes only the CoS value of the outer tag of the encapsulated packet.

Note: Although you configure the command at input, because the switch supports only egress push, this affects only the CoS value of the tag imposed on egress.

- When you configure a policy by entering the match dscp class map configuration command and you enter the set cos-policy-map class configuration command for QinQ EFPs, a DSCP match sets the outer CoS of the encapsulated value.

Note: As in the previous case, the command configured at input affects only the CoS value of the tag imposed at egress.
• You can set DSCP based on matching the outer VLAN.
• If you enter the `match cos` command on EFPs configured for QinQ, the match is to the incoming
  CoS (C-CoS).

The same CoS mapping rules also apply to EFP rewrite operations (see the “Rewrite Operations” section
on page 12-7) when you use the `rewrite ingress tag pop symmetric` service instance command for
VLAN translation.

You can also configure outgoing CoS on an 802.1Q trunk port to simulate CoS mapping.

### 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 (`class`). In the QoS context, the permit and deny actions in the access control entries
(ACEs) have different meanings than do security ACLs. QoS policies do not match ACLs that use the
`deny` keyword.

• If a match with a permit action is encountered (first-match principle), the specified QoS-related
  action is taken.
• 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 an interface, 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 list end.

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. The switch supports MAC ACLs only with destination addresses.

Not all IP ACL options are supported in QoS ACLs. Only these protocols are supported for `permit`
actions in an IP ACL: ICMP, IGMP, GRE, IPINIP, TCP, and UDP. Within a protocol, for IP source and
destination, the switch supports only the source or destination IP address, host, or any. For matching
criteria, the switch supports only DSCP, time-range, and ToS. See the “Using ACLs to Classify Traffic”
section on page 27-35 for more specific information. When you define a class map with the ACL, you
can add the class to a policy.

You can attach a policy that includes unsupported QoS IP ACL options to the target, but QoS ignores the
unsupported options. If you modify an IP ACL in a policy map that is already attached to a target and
the modification causes the policy to become invalid, the policy is detached from the target.

### Classification Based on QoS Groups

A QoS group is an internal label used by the switch to identify packets as a members of a specific class.
The label is not part of the packet header and is restricted to the switch that sets the label and not
communicated between devices. QoS groups provide a way to tag a packet for subsequent QoS action
without explicitly marking (changing) the packet.

A QoS group is identified at ingress and used at egress. It is assigned in an input policy to identify
packets in an output policy. See **Figure 27-3**.
You use QoS groups to aggregate different classes of input traffic for a specific action in an output policy. For example, you can classify an ACL on ingress by using the `set qos-group` command and then use the match `qos-group` command in an output policy.

```
Switch(config)# class-map acl
Switch(config-cmap)# match access-group name acl
Switch(config-cmap)# exit
```

**Input policy map:**
```
Switch(config)# policy-map set-qos-group
Switch(config-pmap)# class acl
Switch(config-pmap-c)# set qos-group 5
Switch(config-pmap-c)# exit
```

**Output policy map:**
```
Switch(config)# policy-map shape
Switch(config-pmap)# class qos-group 5
Switch(config-pmap-c)# shape average 10m
Switch(config-pmap-c)# exit
```

You can use QoS groups to aggregate multiple input streams across input classes and policy maps to have the same QoS treatment on the egress port. Assign the same QoS group number in the input policy map to all streams that require the same egress treatment, and match the QoS group number in the output policy map to specify the required queuing and scheduling actions.

You can also use QoS groups to implement MPLS tunnel mode. In this mode, the output per-hop behavior of a packet is determined by the input EXP bits, but the packet remains unmodified. You match the EXP bits on input, set a QoS group, and then match that QoS group on output to obtain the required QoS behavior.

To communicate an ACL classification to an output policy, you assign a QoS number to specify packets at ingress. This example identifies specific packets as part of QoS group 1 for later processing in an output policy:

```
Switch(config)# policy-map in-gold-policy
Switch(config-pmap)# class in-class1
Switch(config-pmap-c)# set qos-group 1
Switch(config-pmap-c)# exit
```

You use the `set qos-group` command only in an input policy. The assigned QoS group identification is then used in an output policy with no mark or change to the packet. You use the `match qos-group` in the output policy. You cannot configure `match qos-group` for an input policy map.

This example creates an output policy to match the QoS group created in the input policy map `in-gold-policy`. Traffic internally tagged as `qos-group 1` is identified and processed by the output policy.

```
Switch(config)# class-map out-class1
Switch(config-cmap)# match qos-group 1
Switch(config-cmap)# exit
```

The switch supports a maximum of 100 QoS groups.
Classification Based on Discard Class

A discard class is very similar to a QoS group in that it is a virtual packet marking that is carried in the packet within a single device. The difference is that a QoS group defines the complete QoS behavior for a packet, while a discard class only communicates the drop precedence of the packet during congestion management. For example, a packet could be classified on input into one QoS group, but within that QoS group, a policer could mark one of three discard classes, depending on whether the packet was determined to conform to, exceed, or violate the configured specifications. On output, a class would match the QoS group, but you could configure three different drop curves, one for each of the discard classes. The discard class value ranges from 0 to 7.

Classification Based on VLAN IDs

With classification based on VLAN IDs, you can apply QoS policies to frames carried on a user-specified VLAN for a given interface. You can use hierarchical policy maps for per-VLAN classification on trunk ports. Per-VLAN classification is not required on access ports because access ports carry traffic for a single VLAN.

You use the `match vlan vlan-id` class-map configuration command to classify based on the outer VLAN. Use the `match vlan inner vlan-id` class-map configuration command to classify based on the inner VLAN.

QoS-Context Manager

QoS-Context Manager allocates QoS-context for s-vlan and c-vlan matches. To display qos-context manager information use the `show platform qos context struct bridge domain` command.

QOS-contexts are allocated only for intersecting combinations of a configured class-map vlans and the vlans present in encapsulation.

Packets can come from

- Multiple ingress rewrite encapsulation types (pop 0, pop 1 and pop 2)
- With and without Ingress Service policies

For every egress vlan combination, qos-context is allocated in the ingress tcam based on the ingress rewrite type.

Restrictions and limitations

QoS-context manager has the following limitations:

- There are 63 qos-contexts available per bridge-domain.
- QoS-Context manager is fixed and cannot be changed

QoS-context depends on the following:

- Presence of ingress service policy.
- Presence of ingress rewrite type (pop 0, pop 1, pop 2)
- Bridge-domain or xconnect must be configured on the service instance
- Applies to both ME3600X and ME 3800X

Note

Where ingress service policy is not configured the ingress rewrite type is used to allocate qos-contexts.
Working Configuration

The following is an example of a working configuration for allocation of qos-context:

Policy Used:

```
class-map match-any ME-CUSTOMERS-CLASS
match vlan 1500-3299
class-map match-any VOIP-CLASS
match vlan 1201 1301-1302
class-map match-any MGMT-CLASS
match vlan 1050-1099
class-map match-any INTERNET-CLASS
match vlan 1101
bandwidth remaining percent 10
policy-map LLU-NAME-PER-SERVICE-POLICY
class VOIP-CLASS
Priority
class MGMT-CLASS
bandwidth remaining percent 15
class INTERNET-CLASS
bandwidth remaining percent 75
class class-default
bandwidth remaining percent 10
```

Configuration:

```
Switch#sh run int gi0/1
Building configuration...
Current configuration : 336 bytes
!
interface GigabitEthernet0/1
  port-type nni
  switchport trunk allowed vlan none
  switchport mode trunk
  mtu 9216
  service instance 100 ethernet
    encapsulation dot1q 1-1080
    service-policy output LLU-NAME-PER-SERVICE-POLICY
    bridge-domain 3600
  !
End
```

Based on the class-maps in the applied policy, 31 vlans in the class-maps intersecting with the encap vlans "encapsulation dot1q 1-1080" (match vlan 1050-1099)

2 Qos-contexts are allocated for every vlan match in the egress side of this evc, total qos-contexts 31*2=62

Policy is accepted as 63 qos-contexts are supported per bridge-domain

Failed Configuration:

The following is an example of a failed configuration for allocation of qos-contexts:

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface GigabitEthernet0/1
Switch(config-if)# service instance 100 ethernet
Switch(config-if-srv)#encapsulation dot1q 1-1081
QoS: Maximum Egress QosContexts consumed in Bridge-Domain: 3600
QoS: Detaching output service-policy LLU-NAME-PER-SERVICE-POLICY from efp 100
Switch(config-if-srv)#
```

*Apr 21 14:40:37.443: %QOSMGR-3-EQOS_CXT_EXCEEDED: Maximum Egress QosContexts consumed in the Bridge-Domain

*Apr 21 14:40:37.443: %QOSMGR-3-EQOS_CXT_EXCEEDED: Maximum Egress QosContexts consumed in the Bridge-Domain

*Apr 21 14:40:37.443: %QOSMGR-3-EQOS_CXT_EXCEEDED: Maximum Egress QosContexts consumed in the Bridge-Domain
Based on the class-maps in the applied policy, 32 vlans in the class-maps intersecting with the encap vlans "encapsulation dot1q 1-1081" (match vlan 1050-1099)

2 Qos-contexts are allocated for every vlan match in the egress side of this evc, total qos-contexts
32*2=64

Policy is rejected as only 63 qos-contexts are supported per bridge-domain

### Classification for MPLS and EoMPLS

In an MPLS network, QoS can be specified in different ways. For example, the IP precedence field (the first 3 bits of the DSCP field in the header of an IP packet) can specify the QoS value to give the packet. If the network is an MPLS network, the IP precedence bits are copied into the MPLS EXP field at the edge of the network. If a service provider wants 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 27-4 shows an MPLS network that connects two sites of an IP network that belongs to a customer.

**Figure 27-4  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.
Service providers can use MPLS QoS to classify packets according to the type, 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 packet priority 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.

MPLS QoS matches only valid MPLS packets. On input, the match is performed before any label processing on the packet. On output, the match is performed on the final packet after all label operations are performed. See the “Configuring MPLS and EoMPLS QoS” section on page 27-68.

**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 match on Layer 3 parameters (such as IP or DSCP), and Layer 2 parameters (CoS). Mapping does not occur by default and you must set MPLS experimental bits at ingress. See the “Configuring MPLS and EoMPLS QoS” section on page 27-68 for more information about EoMPLS and QoS.

**Policing**

After a packet is classified and assigned a QoS label, you can use policing, as shown in Figure 27-5, to regulate the class of traffic. The policing function limits the amount of bandwidth available to a specific traffic flow or prevents a traffic type from using excessive bandwidth and system resources. A policer identifies a packet as in or out of profile by comparing the rate of the inbound traffic to the configuration profile of the policer and traffic class. Packets that exceed the permitted average rate or burst rate are out of profile or nonconforming. These packets are dropped or modified (marked for further processing), depending on the policer configuration.

Policing is used primarily on receiving interfaces. You can attach a policy map with a policer only in an input service policy. The only policing allowed in an output policy map is in priority queues.

All traffic, whether it is bridged or routed, is subjected to a configured policer. As a result, packets might be dropped or might have the 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 storm-control threshold, preventing storm control from acting on the traffic stream.
Understanding QoS

Figure 27-5 Policing of Classified Packets

You can attach a policy map with a policer only in a service policy. The switch supports 1-rate, 2-color and 2-rate, 3-color ingress policing. Only 1-rate, 2-color policing is supported in egress policies.

For 1-rate, 2-color policing, use the `police` policy map class configuration command to define the policer, the committed rate limitations of the traffic, committed burst size limitations of the traffic, and the action to take for a class of traffic that is below the limits (`conform-action`) and above the limits (`exceed-action`). If you do not specify burst size (`bc`), the system calculates an appropriate burst size value. The calculated value is appropriate for most applications.

When you configure a 2-rate policer, you configure the committed information rate (CIR) for updating the first token bucket, and also the peak information rate (PIR) at which the second token bucket is updated. If you do not configure a PIR, the policer is a standard 1-rate, 2-color policer.

For 2-rate, 3-color policing, you can then choose to set actions to perform on packets that conform to the specified CIR and PIR (`conform-action`), packets that conform to the PIR, but not the CIR (`exceed-action`), and packets that exceed the PIR value (`violate-action`).

- If you set the CIR value equal to the PIR, a traffic rate that is less than or equal to the CIR is in the conform range. Traffic that exceeds the CIR 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.
- If you do not configure a PIR, the policer is configured as a 1-rate, 2-color policer.

Setting the burst sizes too low can reduce throughput in situations with bursty traffic. Setting burst sizes too high can allow too high a traffic rate.

Note

The switch supports byte counters for byte-level statistics for conform, exceed, and violate classes in the `show policy-map interface` privileged EXEC command output.

Use the `service-policy input` interface configuration command to attach the policy map to a physical port or EFP service instance to make it effective. For more information, see the “Attaching a Service Policy to an Interface or EFP” section on page 27-71. Policing is done only on received traffic, so you can only attach a policer to an input service policy.

See the “Configuring a Policy Map with 1-Rate, 2-Color Policing” section on page 27-41 for configuration examples.
You can use the **conform-action**, **exceed-action**, and **violate-action** policy-map class configuration commands or the **conform-action**, **exceed-action**, and **violate-action** policy-map class police configuration commands to specify an action when the packet conforms to or exceeds the specified traffic rates. Conform, exceed, and violate actions are to drop the packet, to send the packet without modifications, to set a new CoS, DSCP, or IP precedence value, or to set a QoS group value for classification at the egress.

You can simultaneously configure multiple conform, exceed, and violate actions for each service class.

### Priority Policing

Priority policing applies only to output policy maps. You can use the **priority** policy map class configuration command in an output policy map to designate a low-latency path or class-based priority queuing for a specific traffic class. With strict priority queuing, the packets in the priority queue are scheduled and sent until the queue is empty. Excessive use of high-priority queuing can create congestion for low priority traffic.

### Restriction and Usage Guidelines

- Apply egress policer on priority queues.
- Egress policer is not supported on vlan classes.
- Egress policer is supported at 3rd level or PHB level only on priority queues.
- Conditional marking is not supported in egress policer.
- 1R3C, 2R3C color blind and color aware policer are not supported.
- mefTCM (color-blind/color-aware w/wo coupling) is not supported.
- Policing at Logical or Physical Level and aggregate policing is not supported.
- 2-Level Hierarchical Policing (color-blind/color-aware) is not supported.
- Strict-priority cannot be configured without a policer, if BW is configured on the same level classes.
- Strict priority cannot co-exist with bandwidth kbps/percent in any other class. For strict priority, configure policer first and then configure bandwidth on the same level classes.

To eliminate this congestion, you can use the Priority with Police feature (priority policing) to reduce the bandwidth used by the priority queue, and allocate traffic rates on other queues. Priority with police is the only form of policing supported in output policy maps.

This example shows how to use the **priority** command with **police** command to configure `out-class1` as the priority queue, with traffic going to the queue that is limited to 20,000,000 bps. so that the priority queue never uses more than that. Traffic above that rate is dropped. This allows other traffic queues to receive some port bandwidth, in this case a minimum bandwidth guarantee of 500,000 and 200,000 kbps. The class-default, queue gets the remaining port bandwidth.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police 200000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth 500000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth 200000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
```
Packet Marking

You can use packet marking in input policy maps to set or modify the attributes for traffic belonging to a specific class. For example, you can change the CoS value in a class or set IP DSCP or IP precedence values for a specific type of traffic. These new values are then used to determine how the traffic should be treated. You can also use marking to assign traffic to a QoS group within the switch.

Traffic marking is typically performed on a specific traffic type at the ingress port. The marking action can cause the CoS, DSCP, or precedence bits to be rewritten or left unchanged, depending on the configuration. This can increase or decrease the priority of a packet in accordance with the policy used in the QoS domain so that other QoS functions can use the marking information to judge the relative and absolute importance of the packet. The marking function can use information from the policing function or directly from the classification function.

Restrictions and Usage Guidelines

- Outer Cos, ipv4 dscp, ipv4 precedence, MPLS EXP marking at egress is supported.
- Multiple marking actions for the same class at egress is supported.
- Egress marking of set cos inner is not supported in Cisco release 15.1(2)EY1a.
- DEI, IPv6 dscp and inner dscp in tunnel is not supported.
- Hierarchical Marking and Enhanced Marking using table-maps is not supported.
- Egress marking cannot be applied to physical classes and vlan classes.
- Qos-group and discard-class marking is not supported at egress, only classification is supported at egress.
- In the case of layer 2 to layer 3 propagation, EXP value is set to 0 by default

Specify and mark traffic by using the `set` commands in a policy map for all supported QoS markings. CoS, IP DSCP, and IP precedence markings are supported in both ingress and egress policies. The task of setting QoS groups is supported only in ingress policies.

Note

The task of setting QoS-groups, discard classes, and imposed EXPs is not supported in egress policies.

A `set` command unconditionally marks the packets that match a specific class. You can then attach the policy map to an interface or service instance as an input policy map or output policy map.

You can simultaneously configure the actions to modify the DSCP, precedence, and CoS markings in the packet for the same service along with the QoS group marking actions. You can use the QoS group number defined in the marking action for egress classification. Figure 27-6 shows the steps involved in marking traffic.

Figure 27-6 Marking Classified Traffic
This example uses a policy map to remark a packet. The first marking (the `set` command) applies to the QoS default class map that matches all traffic not matched by class AF31-AF33 and sets all traffic to an IP DSCP value of 1. The second marking sets the traffic in classes AF31 to AF33 to an IP DSCP of 3.

```
Switch(config)# policy-map Example
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set ip dscp 1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class AF31-AF33
Switch(config-pmap-c)# set ip dscp 3
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy input Example
Switch(config-if)# exit
```

If the egress class match criteria is a part of ingress marking set actions, the egress packet will have both ingress and egress marking action applied on it. If ingress and egress set actions act on the same PHB, the egress set action will take precedence over ingress set action.

In this example, the egress packet is set to both DSCP 20 and CoS 3:

```
Switch(config)# policy-map Ingress Example
Switch(config-pmap)# class dscp 10
Switch(config-pmap-c)# set dscp 20
Switch(config-pmap-c)# exit
Switch(config)# policy-map Egress Example
Switch(config-pmap)# class dscp 10
Switch(config-pmap-c)# set cos 5
Switch(config-pmap-c)# exit
```

### Congestion Avoidance and Queuing

The Congestion Avoidance feature uses algorithms such as tail drop to control the number of packets entering the queuing and scheduling stage to avoid congestion and network bottlenecks. The switch uses WTD and Weighted Random Early Detection (WRED) to manage the queue sizes and provide a drop precedence for traffic classifications.

These sections contain additional information on congestion avoidance and queuing:

- Weighted Tail Drop, page 27-19
- Weighted Random Early Detection (WRED), page 27-21

### Weighted Tail Drop

You set the queue size limits depending on the markings of the packets in the queue. You can assign each packet that travels through the switch to a specific queue and threshold. For example, you can map specific DSCP or CoS values to a specific egress queue and threshold. If the total destination queue size is greater than the threshold of any classified traffic, the next frame of that traffic is dropped.

Figure 27-7 shows an example of WTD operating on a queue with 1000 microseconds worth of data. Three drop percentages are configured: 40 percent (400 microseconds), 60 percent (600 microseconds), and 100 percent (1000 microseconds). These percentages mean that traffic classified to the 40-percent threshold is dropped when the queue depth exceeds 400 microseconds, traffic classified to 60 percent is dropped when the queue depth exceeds 600 microseconds. Traffic up to 400 microseconds can be queued at the 40-percent threshold, up to 600 microseconds at the 60-percent threshold, and up to 1000 microseconds 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.

If the queue is already filled with 600 microseconds worth of data, and a new frame arrives containing CoS values 4 or 5, the frame is subjected to the 60-percent threshold. When this frame is added to the queue, the threshold would be exceeded, so the switch drops it.

You configure WTD by using the `queue-limit` policy-map class command to adjust the queue size (buffer size) associated with a particular class of traffic.

**Note**

Queue-limit is supported only in leaf-level (per-hop behavior) classes.

You specify the maximum threshold in bytes, microseconds or packets. You can specify different queue sizes for different classes of traffic (CoS, DSCP, MPLS EXP, precedence, discard-class, or QoS group) in the same queue. Setting a queue limit establishes a drop threshold for the associated traffic when congestion occurs.

**Note**

You cannot configure queue size by using the `queue-limit` policy map class command without first configuring a scheduling action (bandwidth, shape average, or priority). The only exception to this is when you configure queue-limit for the class-default of an output policy map.

The switch supports up to three unique queue-limit configurations (including the default) across all output policy maps. Within an output policy map, four or eight queues (classes) are allowed, including the class default. Each queue can have three defined thresholds. Only three unique threshold value configurations are allowed per class. Multiple policy maps can share the same queue-limits. Each class-map in a policy-map can either share the same threshold or can have its own unique values.

You can use these same queue-limit values in multiple output policy maps on the switch. However, changing one of the queue-limit values in a class creates a new, unique queue-limit configuration. At any one time, you can attach only three unique queue-limit configurations in output policy maps to targets. If you attempt to attach an output policy map with a fourth unique queue-limit configuration, you see this error message:

`QoS: Configuration failed. Maximum number of allowable unique queue-limit configurations exceeded.`

By default, queues have unique thresholds based on the speed of the interface. You can decrease the queue size for latency-sensitive traffic or increase the queue size for bursty traffic.

Queue bandwidth and queue size (queue limit) are configured separately and are not interdependent. You should consider the type of traffic being sent when you configure bandwidth and queue-limit:

- A large buffer (queue limit) can better accommodate bursty traffic without packet loss, but at the cost of increased latency.
A small buffer reduces latency but is more appropriate for steady traffic flows than for bursty traffic.

Very small buffers are typically used to optimize priority queuing. For traffic that is priority queued, the buffer size usually needs to accommodate only a few packets; large buffer sizes that increase latency are not usually necessary. For high-priority latency-sensitive packets, configure a relatively large bandwidth and relatively small queue size.

WTD thresholds:

- You cannot use the `queue-limit` command to configure more than two threshold values for WTD qualifiers (cos, dscp, precedence, qos-group, discard-class, or mpls experimental). However, there is no limit to the number of qualifiers that you can map to these thresholds.
- You can configure a third threshold value to set the maximum queue by using the `queue-limit` command with no qualifiers.
- You can configure many more WTD thresholds, provided their threshold values are equal to the maximum threshold of the queue provided by the `queue-limit` command.

See the “Configuring Weighted Tail Drop” section on page 27-62.

**Weighted Random Early Detection (WRED)**

WRED combines the capabilities of the RED algorithm with the IP Precedence feature to enable preferential traffic handling of high-priority packets. WRED can selectively discard low-priority traffic when the switch begins to get congested, and provide differentiated egress drop thresholds based on the DSCP, IP precedence, CoS values, or MPLS EXP bits.

You can configure WRED to ignore IP precedence when making drop decisions so that non-weighted RED behavior is achieved.

WRED attempts to anticipate and avoid congestion rather than control congestion after it occurs.

WRED works with ipv6 dscp/class of service.

**Why Use WRED?**

WRED facilitates early detection of congestion and enables multiple classes of traffic. It also protects against global synchronization. For these reasons, WRED is useful on any output interface on which you expect congestion to occur.

However, WRED is usually used in the core routers of a network rather than at the edge of a network. Edge routers assign IP precedences to packets as they enter the network. WRED uses these precedences to determine how to treat different types of traffic.

WRED provides separate thresholds and weights for different IP precedences, allowing you to provide different qualities of service with regard to packet dropping for different traffic types. Standard traffic can be dropped more frequently than premium traffic during periods of congestion.

**How It Works**

By randomly dropping packets prior to periods of high congestion, WRED communicates with the packet source to decrease its transmission rate. If the packet source is using TCP, it will decrease its transmission rate until all the packets reach their destination, which indicates that the congestion is cleared.

WRED generally drops packets selectively, based on IP precedence. Packets with a higher IP precedence are less likely to be dropped than packets with a lower precedence. Thus, the higher the priority of a packet, the higher the probability that the packet will be delivered.
Understanding QoS

WRED reduces the chances of tail drop by selectively dropping packets when the output policy maps begin 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 and minimizes the chances of global synchronization. Thus, WRED allows the transmission line to be used fully at all times.

In addition, WRED statistically drops more packets from large users than from small users. Therefore, traffic sources that generate the most traffic are more likely to be slowed down than traffic sources that generate less traffic.

WRED avoids the globalization problems that occur when tail drop is used as the congestion avoidance mechanism. Global synchronization manifests when multiple TCP hosts reduce their transmission rates in response to packet dropping, and increase their transmission rates once again when the congestion is reduced.

WRED is useful only when the bulk of the traffic is TCP/IP traffic. With TCP, dropped packets indicate congestion. Therefore the packet source will reduce its transmission rate. With other protocols, packet sources may not respond or may resend dropped packets at the same rate. Thus, dropping packets does not decrease congestion.

WRED treats non-IP traffic as precedence 0, the lowest precedence. Therefore, non-IP traffic, in general, is more likely to be dropped than IP traffic.

Figure 27-8 illustrates how WRED works.

**Figure 27-8  How WRED works.**

![Diagram of WRED process]

**Average Queue Size**

The router automatically determines the parameters to be used in WRED calculations. The average queue size is based on the previous average and the current size of the queue. The formula is:

\[
\text{average} = (\text{old\_average} \times (1 - 2^{-n})) + (\text{current\_queue\_size} \times 2^{-n})
\]

where \( n \) is the exponential weight factor, a user-configurable value. The default value of the exponential weight factor is 9. We recommend that you use only the default value for the exponential weight factor. Change this value from the default value only if you have determined that your scenario will benefit from using a different value.
For high values of $n$, the previous average becomes more important. A large factor smooths out the peaks and lows in queue length. The average queue size is unlikely to change very quickly, avoiding drastic swings in size. The WRED process will be slow to start dropping packets, but it may continue dropping packets for a time after the actual queue size has fallen below the minimum threshold. The slow-moving average will accommodate temporary bursts in traffic.

**Note**

If the value of $n$ gets too high, WRED will not react to congestion. Packets will be sent or dropped as if WRED were not in effect.

For low values of $n$, the average queue size closely tracks the current queue size. The resulting average may fluctuate with changes in the traffic levels. In this case, the WRED process responds quickly to long queues. After the queue falls below the minimum threshold, the process will stop dropping packets.

If the value of $n$ gets too low, WRED will overreact to temporary traffic bursts and drop traffic unnecessarily.

See the “Configuring Weighted Random Early Detection” section on page 27-64.

**Congestion Management and Scheduling**

MQC provides several related mechanisms in output policy maps to control outgoing traffic flow. The scheduling stage holds packets until the appropriate time to send them to one of the four or eight traffic queues. Queuing assigns a packet to a particular queue based on the packet class and is enhanced by the WTD algorithm for congestion avoidance. You can use different scheduling mechanisms to provide a guaranteed bandwidth to a particular class of traffic while also serving other traffic in a fair way. You can limit the maximum bandwidth that can be consumed by a particular class of traffic and ensure that delay-sensitive traffic in a low-latency queue is sent before traffic in other queues.

The switch supports these scheduling mechanisms:

- **Traffic shaping**
  
  You use the `shape average` policy map class configuration command to specify that a class of traffic should have a maximum permitted average rate. You specify the maximum rate in bits per second.

- **Class-based-weighted-fair-queuing (CBWFQ)**
  
  You can use the `bandwidth` policy-map class configuration command to control the bandwidth allocated to a specific class. Minimum bandwidth can be specified as a bit rate, or as a percentage of total bandwidth, or as remaining bandwidth.

- **Priority queuing or class-based low-latency scheduling**
  
  You use the `priority` policy-map class configuration command to specify that a class of traffic has low latency requirements with respect to other classes. When you configure this command in a class, you cannot configure bandwidth in any other child class associated with the same parent.

These sections contain additional information about scheduling:

- **Traffic Shaping**, page 27-24
- **Class-Based Weighted Fair Queuing**, page 27-26
- **Priority Queuing**, page 27-26
Traffic Shaping

Traffic shaping or class-based peak rate scheduling is used to specify the maximum transmission rate for a traffic class. Unlike traffic policing, where nonconforming packets are dropped or marked right away, packets exceeding the rate specified in the shape command are usually buffered and can be sent later when bandwidth is available. While policing propagates traffic bursts, shaping smooths bursts by sending the packets later. Traffic policing is used in input policy maps, and traffic shaping occurs as traffic leaves an interface or service instance.

Configuring a queue for traffic shaping sets the maximum bandwidth or PIR of the queue. You can set the PIR from 1 Kb/s to 10 Gb/s. You can also configure the PIR as a percentage of the PIR of a parent level.

Note

You cannot configure traffic shaping (shape average) and or priority queuing (priority) for the same class in an output policy map. However, you can configure CIR, PIR, and EIR bandwidth independently for a class and use the bandwidth, bandwidth remaining, and shape average commands at the same time within a class.

Class-Based Shaping

Class-based shaping uses the shape average policy-map class configuration command to limit the rate of data transmission in bits per second to be used for the committed information rate for a class of traffic. The switch supports separate queues for four or eight classes of traffic, including the default queue for class class-default, unclassified traffic.

See the “Configuring Class-Based Shaping” section on page 27-54.

Port Shaping

Port shaping is applied to all the traffic leaving a target. It uses a policy map with only class default when you specify the maximum bandwidth for a port using the shape average command. You can attach a child policy to the class default in a hierarchical policy map format to specify class-based and VLAN-based actions.

Where EFPs are configured to aggregately shape the EFPs in a port, configure a port policy using a class-default shaper configuration.

See the “Configuring Port Shaping” section on page 27-55.

Restriction and Usage Guidelines

- To allow coexistence, apply policy-map on the main interface before applying the policy-map on the sub targets.
- You can configure port level shaping with these policy-maps:
  - Flat policy-map on the service instance.
  - HQoS policy-map on the service instance.
- Port level shaping is supported in the egress direction on the main interface.
- Only Class-default is supported on the port-shaper policy-map.
- EVC QoS is not allowed for user defined classes on the main interface policy-map, or if there is a HQoS policy-map on the main interface.
- Summation of Bandwidth configured on the polices applied on service instances should not exceed the port-shaper value.
• Shape configured on the polices applied on service instance should not exceed the port-shaper value.
• It is recommended to remove the policy-map on the main interface only after removing policy-maps on the service instances.
• It is recommended to apply the policy-map on the main interface before adding the policy-maps on the service instances.
• It is recommended not to change the port-shaper values dynamically when QoS policy-maps are applied.
• Below are the list of unsupported configuration.
  – Port policy(class-default shaper + PHB classes) and policies on EFPs
  – Port policy(class-default shaper + Vlan classes) and policies on EFPs
  – Port policy(class-default shaper + Vlan + PHB classes) and policies on EFPs
  – Port policy(PHB classes) and policies on EFPs
  – Port policy(Vlan classes) and policies on EFPs
  – Port policy(Vlan + PHB classes) and policies on EFPs
  – Port policy(class based policies) to handle LLQ across EFPs + EFP policies
  – Match efp-id on the port policy

Parent-Child Hierarchy

The switch also supports parent policy levels and child policy levels for traffic shaping. The QoS parent-child structure is used for specific purposes when a child policy is referenced in a parent policy to provide additional control of a specific traffic type.

Note
The total of the minimum bandwidth guarantees (CIR) for each queue of the child policy cannot exceed the total port-shape rate.

This is an example of a parent-child configuration:

```
Switch(config)# policy-map parent
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 50000000
Switch(config-pmap-c)# service-policy child
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output parent
Switch(config-if)# exit
```

You can also configure the PIR in a child policy to be an absolute rate calculated as a percentage of the PIR of the parent level policy. You can configure the child PIR from 0 percent to 100 percent of the parent policy.

```
Switch(config)# policy-map child
Switch(config-pmap)# class class2
Switch(config-pmap-c)# shape average percent 50
Switch(config-pmap-c)# exit
```
Class-Based Weighted Fair Queuing

You can configure class-based weighted fair queuing (CBWFQ) to set the relative precedence of a queue by allocating a portion of the total bandwidth that is available for the port. You use the `bandwidth` policy-map class configuration command to set the minimum guaranteed output bandwidth or CIR for a class of traffic as a rate (kilobits per second), a percentage of total bandwidth, or a percentage of remaining bandwidth.

### Note
When you configure bandwidth in a policy map, you must configure all rates in the same format, either a configured rate or a percentage. The total of the minimum bandwidth guarantees (CIR) for each queue of the policy cannot exceed the total speed of the parent.

- Configuring bandwidth for a class of traffic as an absolute rate (kilobits per second) or a percentage of total bandwidth represents the minimum bandwidth guarantee (the CIR) for that traffic class. This means that the traffic class gets at least the bandwidth indicated by the command, but is not limited to that bandwidth. Any excess bandwidth on the port is allocated to each class in the same ratio in which the CIR rates are configured. The CIR range is from 1 Kb/s to 10 Gb/s or 1 to 100 percent.

You configure the `bandwidth percent` command mainly in hierarchical policy maps where a child CIR guarantee is tied to the parent CIR guarantee.

The sum of all CIR commitments for a set of peer classes cannot exceed the PIR (shape) of the parent level. A queue without a configured CIR commitment does not receive any committed bandwidth in the scheduler and can be entirely superseded other classes. If CIR bandwidth is required for any class, including class-default, you must configure it.

### Note
You cannot configure bandwidth as an absolute rate or a percentage of total bandwidth when `priority` is configured for another class in the output policy. However, you can configure CIR, EIR, and PIR independently for a class and use the `bandwidth`, `bandwidth remaining`, and `shape average` commands, respectively, at the same time within a class.

- Configuring bandwidth as a percentage of remaining bandwidth determines the portion of the excess bandwidth of the target that is allocated to the class. This means that the class is allocated bandwidth only if there is excess bandwidth on the target and if there is no minimum bandwidth guarantee for this traffic class. By default, the total excess bandwidth is divided equally among the classes. You can configure bandwidth as remaining percentage to configure an unequal distribution for prioritizing classes. The total bandwidth that you can allocate between peer classes is 100 percent.

### Note
You cannot configure bandwidth as percentage of remaining bandwidth when `priority` is configured for another class in the output policy map.

For more information, see the “Configuring Class-Based-Weighted Fair Queuing” section on page 27-51.

Priority Queuing

You can use the `priority` policy-map class configuration command to ensure that a particular class of traffic is given preferential treatment with respect to other classes associated with the same parent entity. With priority queuing, the priority queue is constantly serviced until the queue is empty. With priority queuing, traffic for the associated class is sent before packets in other queues are sent.
When you configure priority in a class, you cannot configure the bandwidth command in any other sibling class associated with the same parent.

**Note**  
You should exercise care when using the `priority` command. Excessive use of strict priority queuing might cause congestion in other queues.

Priority queuing has these restrictions:

- You can associate the `priority` command with a single unique class for each policy map.
- You cannot configure priority and any other scheduling action (`shape average` or `bandwidth`) in the same class.
- You cannot configure priority queuing for the `class-default` of an output policy map.

For more information, see the “Configuring Class-Based Priority Queuing” section on page 27-60.

**Input and Output Policy Maps**

Policy maps are either input policy maps or output policy maps applied to packets as they enter or leave the switch by service policies attached to targets. Input policy maps perform policing and marking on received traffic. Policed packets are dropped or reduced in priority (marked down) if they exceed the maximum permitted rates. Output policy maps perform scheduling and queuing on traffic as it leaves the switch.

Input policies and output policies have the same basic structure but differ in the characteristics that they regulate. Figure 27-9 shows the relationship of input and output policies.

**Figure 27-9 Input and Output Policy Relationship**

Traffic received on a port or service instance → Classification → Policing → Mark → Queueing and scheduling

Classification:
- Inspect packet, and process the `match` commands.

Policing:
- Compare received traffic rate with the configured policer and determine if the packet is in profile or out of profile.

Mark:
- Based on whether the packet is in or out of profile and the configured parameters, determine whether to pass through, mark down, or drop the packet.

Queueing and scheduling:
- Based on the hierarchical QoS configuration, create queues for classes, VLANs, and physical interfaces. Place the packet into the queue and service it according to the configuration.
Input policy map classification criteria include matching CoS, DSCP, IP precedence, or MPLS EXP values or matching an ACL or VLAN ID (for per-port, per-VLAN QoS). Input policy maps support two actions: marking and policing. You can specify these actions in any one level of the hierarchical policy.
map, but actions cannot be nested. That is, if a child policy has a policer, then the parent policy map cannot have a policer. Likewise, if there is marking in a child policy, there cannot be marking in a parent policy.

Only input policies provide matching on access groups, and only output policies provide matching on QoS groups and discard classes. The class **class-default** is used in a policy map for any traffic that does not explicitly match any other class in the policy map. Input policy maps do not support queuing and scheduling keywords, such as **bandwidth**, **queue-limit**, **priority**, and **shape average**.

**Output Policy Maps**

Output policy map classification criteria include matching CoS, DSCP, an IP precedence, MPLS EXP, or QoS groups, or a discard-class value. Output policy maps can have any of these actions:

- Queuing (**queue-limit**)
- Scheduling (**bandwidth**, **priority**, and **shape average**)

Policies attached to an EFP support only 2-level scheduling. Although you can attach a 3-level hierarchical policy to an EFP, the policy should conform to these rules:

- Only two or the three levels can have a scheduling action (bandwidth, priority, or shape).
- One of the two levels must be the class (bottom-most) level.

Output policy maps do not support matching of access groups. You can use QoS groups as an alternative by matching the appropriate access group in the input policy map and setting a QoS group. In the output policy map, you can then match the QoS group. See the “Classification Based on QoS Groups” section on page 27-10 for more information.

- A class-level policy (a child policy with class maps matching CoS, DSCP, IP precedence, MPLS EXP, QoS group, or discard-class) can have a maximum of eight classes including class default.
- A VLAN-level policy (a parent policy that has classes matching VLANs) can have a maximum of 4000 classes, including class default.
- A physical-level policy can have only class-default in the entire policy map.

You can attach an output policy map to any or all targets on the switch. The switch supports configuration and attachment of a unique output policy map for each port or service instance.

However, these output policy maps can contain only three unique configurations of queue limits. These three unique queue-limit configurations can be included in as many output policy maps as there are switch ports. There are no limitations on the configurations of bandwidth, priority, or shaping.

**QoS Treatment for Performance-Monitoring Protocols**

QoS is not configurable for Cisco IP service level agreements (IP SLA) probes or for traffic to the CPU. QoS treatment is set by default.

- **Cisco IP-SLAs Probes**, page 27-29
- **CPU Traffic**, page 27-30

**Cisco IP-SLAs Probes**

For information about Cisco IP service level agreements (IP SLAs), see the “Understanding Cisco IOS IP SLAs” section on page 33-1.
The QoS treatment for IP-SLA probes exactly reflects effects that occur to the normal data traffic crossing the device. The generating device does not change the probe markings. It queues these probes based on the configured queueing policies for normal traffic.

- **Marking**
  - By default, the CoS marking of CFM traffic (including IP SLAs using CFM probes) is not changed. QoS configuration cannot change this behavior.
  - By default, IP traffic marking and the CoS marking of all other Layer 2 non-IP traffic is not changed. The QoS marking feature can change this behavior.

- **Queuing**
  - IP SLAs traffic is queued according to its ToS or DSCP value and the output policy map configured on the egress target, similarly to normal traffic. QoS cannot change this behavior.
  - By default, all other Layer 2 non-IP traffic and all IP traffic is statically mapped to a queue on the egress target.

**CPU Traffic**

By default, the switch assigns a separate classifier, CPU-traffic classifier, for all traffic destined to the CPU. For traffic from the CPU, the switch uses a default classifier for high-priority control protocol traffic. These protocols are considered high priority:

- Protocols with the PAK_PRIORITY flag set in Cisco IOS software. These include EIGHT, HSPR, GRD, LDP, OSPF, RIP, WCCP, BFD, CFM, SAA, CDP, ISIS, DTP, IGRP, Ethernet OAM, LACP, LLDP, PAgP, and STP.
- IP protocols with IP precedence set to 6 or 7.

All other traffic from the CPU is classified with a normal classifier.

**Configuring QoS**

- Default QoS Configuration, page 27-30
- Configuration Guidelines and Limitations, page 27-31
- Configuring Input Policy Maps, page 27-32
- Configuring Output Policy Maps, page 27-48
- Configuring MPLS and EoMPLS QoS, page 27-68
- Attaching a Service Policy to an Interface or EFP, page 27-71

**Default QoS Configuration**

There are no policy maps, class maps, table maps, or policers configured. At the egress target, all traffic goes through a single default queue that is given the full operational bandwidth.

The packets are not modified. The CoS, DSCP, IP precedence, and MPLS EXP values in the packet are not changed. Traffic is switched in pass-through mode without any rewrites and classified as best effort without any policing.
Configuration Guidelines and Limitations

The ME 3800X and ME 3600X switches support the same QoS functionality. All switches support a total of 4,000 QoS instances, where a QoS instance is any target on which a QoS per-hop behavior policy is attached. A target can be a port, a VLAN class, or an EFP service instance.

- You can configure a maximum of 1024 policy maps.
- You can apply one input policy map and one output policy map to an interface or service instance.
- The maximum number of classification criteria per class map is 64. The maximum number of classes per policy map is 4000.
- Policy configurations are validated as they are configured. When invalid configurations are detected, they are rejected. In some cases the configuration cannot be validated until it is associated with an interface.
- If you modify a feature characteristic on a port or EFP that has a policy map attached and the new configuration makes the policy map invalid, the attached policy is automatically detached.
- You can attach service policies to switchports, routed ports, or EFPs. However, you cannot attach a service policy to a physical port that is configured with service instances (EFPs) and you cannot attach service policies to switch virtual interfaces (SVIs).
- You cannot attach a service policy to an EtherChannel. You can only attach service policies to individual ports in the port channel. You cannot attach a service policy to an EFP that belongs to a port channel interface.
- When a configured policer rate, policer burst-size, or queue-rate cannot be achieved in hardware within 1 percent, the configuration is rejected.
- Egress classification for a class of traffic that has been acted on by an input policy-map can take place only on the per-hop behavior criteria and value established by the input policy-map.
  - If a class in an input policy-map is classifying based on per-hop behavior criteria and is configured for policing but not marking, then the per-hop behavior established by the input policy-map for that class of traffic is the classification criteria and value in the associated class-map.
  - If a class in an input policy-map is not classifying on per-hop behavior criteria, but is classifying on flow criteria by using a MAC ACL or IP ACL, and it is configured for policing, a default best-effort per-hop behavior is established for that class of traffic. Traffic in this class is not eligible for egress classification based on per-hop behavior criteria.
  - If a class in an input policy-map is configured for marking, the per-hop behavior established by the input policy-map for that class of traffic is the marked per-hop behavior criteria and value.
  - If a class in an input policy-map is not configured for any action (class-default), a default best-effort per-hop behavior is established for that class of traffic. Traffic in this class is not eligible for egress classification based on PHB-criteria.

For example: if the per-hop behavior established for a class of traffic by an input policy-map is DSCP ef, you can classify that class of traffic on the egress based only on DSCP ef and not on any other mutually exclusive per-hop behavior such as outer CoS or inner CoS.

- Egress classification on a target with no input policy map attached can use any classification criteria specified in the egress policy. When an input policy map is attached to a target, even if traffic does not match any classes in the input policy, it cannot be egress-classified.
- When configuring both MPLS VPN and QoS, you can apply most 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 traffic that matches traffic based on DSCP or MPLS. For information about configuring QoS with MPLS and EoMPLS, see the “Configuring MPLS and EoMPLS QoS” section on page 27-68.

- There is a limitation per bridge-domain on the number of unique flows classified on inner or outer VLANs that you can configure for egress classification. An error message appears when this limitation is exceeded.
- Hierarchical marking and policing are not supported. You can configure marking and policing for any number of classes on any one of the three levels of the policy-map hierarchy. If you configure marking on one level, you can configure policing without marking (transmit, drop) on another level.
- An EFP can support only 2-level egress scheduling policies. If you attach a 3-level hierarchical policy to an EFP, only 2 of the 3 levels can have scheduling actions (bandwidth, shape, or priority).
- There is a limitation on the maximum number of unique per-hop behavior-criteria combinations that can be configured on the system. The limit is internally calculated and is a function of input classification, marking, and egress classification based on per-hop behavior. An error message appears when this limit is reached.

Configuring Input Policy Maps

- Configuring Input Class Maps, page 27-32
- Using ACLs to Classify Traffic, page 27-35
- Configuring Class-Based Marking, page 27-39
- Configuring Policing, page 27-41

Configuring Input Class Maps

You use the `class-map` command to name and to isolate a specific traffic flow (or class) from all other traffic. A class map defines the criteria to use to match against a specific traffic flow to further classify it. You define match criteria with one or more `match` statements entered in the class-map configuration mode. Match statements can include criteria such as an ACL, inner or outer CoS value, DSCP value, IP precedence values, MPLS experimental labels, or inner or outer VLAN IDs.

In an input policy, the match criteria acts on the packet on the wire before any VLAN-mapping rewrite operations on ingress.
Beginning in privileged EXEC mode, follow these steps to create a class map and to define the match criterion to classify traffic:

<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>class-map [match-all</td>
<td>match-any] class-map-name</td>
</tr>
<tr>
<td></td>
<td>Create a class map, and enter class-map configuration mode. By default, no class maps are defined.</td>
</tr>
<tr>
<td></td>
<td>• For class-map-name, specify the name of the class map.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) Use the match-all keyword to perform a logical AND of all matching statements under this class map. All match criteria in the class map must be matched.</td>
</tr>
<tr>
<td></td>
<td>Note  The match-all keyword is supported only for outer VLAN and inner VLAN or outer CoS and inner CoS matches for QinQ packets. The match-all keyword is rejected for all other mutually exclusive match criteria.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) Use the match-any keyword to perform a logical OR of all matching statements under this class map. One or more match criteria must be matched.</td>
</tr>
</tbody>
</table>
### Chapter 27 Configuring Quality of Service (QoS)

#### Configuring QoS

**Step 3**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`match {access-group acl-index-or-name</td>
<td>cos-cos-list</td>
</tr>
<tr>
<td></td>
<td>For <code>access-group acl-index-or-name</code>, specify the number or name of an ACL. Matching access groups is supported only in input policy maps.</td>
</tr>
<tr>
<td></td>
<td>• Enter <code>cos cos-list</code> to match a packet based on the outer VLAN tag or the service-provider CoS value. You can specify up to four Layer 2 CoS values to match against the packet. Separate each value with a space. The range is 0 to 7.</td>
</tr>
<tr>
<td></td>
<td>• Enter <code>cos inner cos-list</code> to match a packet based on the inner CoS value. For packets only one tag, this command has no effect. You can specify up to four Layer 2 CoS values to match against the packet. Separate each value with a space. The range is 0 to 7.</td>
</tr>
<tr>
<td></td>
<td>• For <code>ip dscp dscp-list</code>, enter a list of up to eight IPv4 DSCP values to match against incoming packets. Separate each value with a space. You can enter multiple <code>dscp-list</code> lines to match more than eight DSCP values. The numerical range is 0 to 63. You can also configure DSCP values in other forms (af numbers, cs numbers, <code>default</code>, or <code>ef</code>).</td>
</tr>
<tr>
<td></td>
<td>• For <code>ip precedence ip-precedence-list</code>, enter a list of up to four IPv4 precedence values to match against incoming packets. Separate each value with a space. You can enter multiple <code>ip-precedence-list</code> lines to match more than four precedence values. The range is 0 to 7.</td>
</tr>
<tr>
<td></td>
<td>• For <code>mpls experimental topmost value</code>, enter a list of up to eight MPLS experimental labels. You can enter multiple lines to match more than eight MPLS experimental values. This keyword matches only valid MPLS packets. Separate each value with a space. The range is 0 to 7.</td>
</tr>
<tr>
<td></td>
<td>• Enter <code>vlan vlan-id</code> to match a packet based on the outermost, service-provider VLAN ID (S-VLAN). For untagged packets, this matches the default VLAN associated with the packets from the port or EFP. You can enter a single VLAN ID or a range of VLANs separated by a hyphen. The range is from 1 to 4095.</td>
</tr>
<tr>
<td></td>
<td>• Enter <code>vlan inner vlan-id</code> to match a packet based on the C-VLAN, the inner customer VLAN ID of an 802.1Q tunnel. For packets with only one tag, the command has no effect. You can specify a single VLAN identified by a VLAN number or a range of VLANs separated by a hyphen. The range is 1 to 4094.</td>
</tr>
</tbody>
</table>

**Step 4**

<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 5**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show class-map</code></td>
<td>Verify your entries.</td>
</tr>
</tbody>
</table>

**Step 6**

<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>

Use the **no** form of the appropriate command to delete an existing class map or remove a match criterion.
This example shows how to create access list 103 and 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.

Switch(config)# access-list 103 permit 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 incoming traffic with DSCP values of 10, 11, and 12.

Switch(config)# class-map match-any 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 incoming traffic with IP-precedence values of 5, 6, and 7:

Switch(config)# class-map match-any class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# exit

This example shows how to create a class-map called parent-class, which matches incoming traffic with VLAN IDs in the range from 30 to 40.

Switch(config)# class-map match-any parent-class
Switch(config-cmap)# match vlan 30-40
Switch(config-cmap)# exit

Using ACLs to Classify Traffic

You can classify IP traffic by using IP standard or IP extended ACLs. You can classify IP and non-IP traffic by using Layer 2 MAC ACLs. For more information about configuring ACLs, see the chapter on “Configuring Network Security with ACLs” in the software configuration guide.

QoS policies match only the permit keyword. Not all ACL criteria are supported for QoS classification. Note the available keywords in the procedures.

You can attach a policy that includes unsupported QoS IP ACL options to the target, but QoS ignores the unsupported options. If you modify an IP ACL in a policy map that is already attached to a target and the modification causes the attached policy to become invalid, the policy is detached from the target.

- “Creating IP Standard ACLs” section on page 27-36
- “Creating IP Extended ACLs” section on page 27-36
- “Creating Layer 2 MAC ACLs” section on page 27-38
Creating IP Standard ACLs

Beginning in privileged EXEC mode, follow these steps to create an IP standard ACL for IP traffic:

<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>access-list access-list-number permit 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>or</td>
<td>ip access-list standard name</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show access-lists</td>
</tr>
<tr>
<td>Step 5</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.

```
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
```

Creating IP Extended ACLs

Although you can configure many options in ACLs, only some are supported for QoS ACLs.

• For permit protocol, the supported keywords are: gre, icmp, igmp, ipinip, tcp, and udp.
• For source and destination address, the supported entries are ip-address, any, or host.
• For match criteria, the supported keywords are dscp or tos. You can also specify a time-range.
Beginning in privileged EXEC mode, follow these steps to create an IP extended ACL for 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></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>access-list access-list-number permit protocol {source source-wildcard destination destination-wildcard} [tos tos] [dscp dscp] [time-range name]</td>
</tr>
<tr>
<td></td>
<td>Create an IP extended ACL. Repeat the step as many times as necessary.</td>
</tr>
<tr>
<td></td>
<td>- For access-list-number, enter the access list number. The range is 100 to 199 and 2000 to 2699.</td>
</tr>
<tr>
<td></td>
<td>- Always use the <strong>permit</strong> keyword for ACLs used as match criteria in QoS policies. QoS policies do not match <strong>deny</strong> ACLs.</td>
</tr>
<tr>
<td></td>
<td>- For protocol, enter the name or number of an IP protocol. Although other protocols are visible in the command-line help, only these are supported: IGMP, TCP, UPD, ICMP, IPINIP, and GRE. If you enter other protocol types, the command is rejected.</td>
</tr>
<tr>
<td></td>
<td>- The <strong>source</strong> is the number of the network or host sending the packet.</td>
</tr>
<tr>
<td></td>
<td>- The <strong>source-wildcard</strong> applies wildcard bits to the source.</td>
</tr>
<tr>
<td></td>
<td>- The <strong>destination</strong> is the network or host number receiving the packet.</td>
</tr>
<tr>
<td></td>
<td>- The <strong>destination-wildcard</strong> applies wildcard bits to the destination.</td>
</tr>
<tr>
<td></td>
<td>You can specify source, destination, and wildcards as:</td>
</tr>
<tr>
<td></td>
<td>- The 32-bit quantity in dotted-decimal format.</td>
</tr>
<tr>
<td></td>
<td>- The keyword <strong>any</strong> for 0.0.0.0 255.255.255.255 (any host).</td>
</tr>
<tr>
<td></td>
<td>- The keyword <strong>host</strong> for a single host 0.0.0.0.</td>
</tr>
<tr>
<td></td>
<td>Although other optional keywords are visible and can be configured, only these are supported in QoS ACLs:</td>
</tr>
<tr>
<td></td>
<td>- <strong>tos</strong>—Enter to match by type of service level, specified by a number from 0 to 15 or a name: <strong>normal</strong> (0), <strong>max-reliability</strong> (2), <strong>max-throughput</strong> (4), <strong>min-delay</strong> (8).</td>
</tr>
<tr>
<td></td>
<td>- <strong>dscp</strong>—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.</td>
</tr>
<tr>
<td></td>
<td>- <strong>time-range</strong>—Specify a configured time range for applying the ACLs. You configure the time range using the <strong>time-range</strong> <strong>time-range-name</strong> global configuration command.</td>
</tr>
<tr>
<td>or</td>
<td>ip access-list extended name</td>
</tr>
<tr>
<td></td>
<td>Define an extended IPv4 access list using a name, and enter access-list configuration mode. The <strong>name</strong> can be a number from 100 to 199.</td>
</tr>
<tr>
<td></td>
<td>In access-list configuration mode, enter <strong>permit protocol {source source-wildcard destination destination-wildcard} [tos tos] [dscp dscp] [time-range name]</strong> as defined in Step 2.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show access-lists</td>
</tr>
<tr>
<td></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 5</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 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 ToS value of 5:

```
Switch(config)# access-list 100 permit ip host 10.1.1.1 host 10.1.1.2 tos 5
```

### Creating Layer 2 MAC ACLs

Beginning in privileged EXEC mode, follow these steps to create a Layer 2 MAC ACL for non-IP traffic:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>&lt;br&gt;configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong>&lt;br&gt;mac access-list extended name</td>
<td>Create a Layer 2 MAC ACL by specifying the name of the list and enter extended MAC ACL configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong>&lt;br&gt;permit [any</td>
<td>host dst-MAC-addr</td>
</tr>
<tr>
<td><strong>Note</strong>&lt;br&gt;Although visible in the command-line help, the <code>host src-MAC-addr mask</code> keywords are not supported.</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>&lt;br&gt;end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong>&lt;br&gt;show access-lists [access-list-number</td>
<td>access-list-name]</td>
</tr>
<tr>
<td><strong>Step 6</strong>&lt;br&gt;copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

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 a `permit` statement that allows traffic from the host with MAC address 0001.0000.0001 to the host with MAC address 0002.0000.0001:

```
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)# exit
```
Configuring Class-Based Marking

You use the `set` policy-map class configuration command to set or modify the attributes for traffic belonging to a specific class.

Follow these guidelines when configuring class-based marking:

- Hierarchical marking is not supported.
- You can configure marking for any number of classes on any of the three levels of policy map hierarchy. If you configure marking on one level, you can configure policing without marking (transmit, drop) on another level.

In the privileged EXEC mode, perform these steps to create an input policy map that marks traffic,

<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 policy-map configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>`class {class-map-name</td>
<td>class-default}`</td>
</tr>
</tbody>
</table>
Chapter 27  Configuring Quality of Service (QoS)

Configuring QoS

Step 4

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>set { cos cos_value | discard-class value | [ip] dscp dscp_value | [ip] precedence precedence_value | mpls experimental { imposition | topmost} experimental _value | qos-group value }</td>
<td>Mark traffic by setting a new value in the packet, specifying a table map, or specifying a QoS group.</td>
</tr>
<tr>
<td>• For cos cos_value, enter a new CoS value to be assigned to the classified traffic. The range is 0 to 7.</td>
<td></td>
</tr>
<tr>
<td>• For discard-class value, enter the exact value to be marked for traffic to be discarded. The range is 0 to 7.</td>
<td></td>
</tr>
<tr>
<td>• For [ip] dscp new-dscp, enter a new DSCP value to be assigned to the classified traffic. The range is 0 to 63 or valid af numbers, cs numbers, default, or ef.</td>
<td></td>
</tr>
<tr>
<td>• For [ip] precedence new-precedence, enter a new IP-precedence value to be assigned to the classified traffic, 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).</td>
<td></td>
</tr>
<tr>
<td>Note  A class can have either DSCP or precedence marking. If one of these is already configured in a class and you configure the other keyword, the newer command overwrites the previous command. If the value configured for a set ip precedence class in an earlier class in a policy overlaps the value configured for a set ip dscp class in a later class, then the earlier configuration is always matched.</td>
<td></td>
</tr>
<tr>
<td>• For mpls experimental imposition exp-number, enter the new MPLS experimental value to be set at tag imposition. This keyword specifies that the MPLS experimental value in a packet header is set with the new value after the packet is switched. This keyword applies only to MPLS packets that are MPLS routed. The range is 0 to 7.</td>
<td></td>
</tr>
<tr>
<td>• mpls experimental topmost exp-number, enter the new MPLS experimental value for the outermost or topmost label. This keyword marks all valid MPLS packets. The range is 0 to 7.</td>
<td></td>
</tr>
<tr>
<td>• For qos-group value, identify a QoS group to be used at egress to identify specific packets. The range is from 0 to 99.</td>
<td></td>
</tr>
</tbody>
</table>

If the policy is already attached to an interface, you must exit policy-map class configuration mode before the modification is applied.

Step 5

end  Return to privileged EXEC mode.

Step 6

show policy-map [policy-map-name [class class-map-name]]  Verify your entries.

Step 7

copy running-config startup-config  (Optional) Save your entries in the configuration file.

After you create the input policy map, attach it to a target. See the “Attaching a Service Policy to an Interface or EFP” section on page 27-71. Use the no form of the appropriate command to delete a policy map or remove an assigned CoS, DSCP, MPLS, precedence, or QoS-group value.
This example uses a policy map to remark a packet. The first marking (the set command) applies to the 
QoS default class map that matches all traffic not matched by class AF31-AF33 and sets all traffic to an 
IP DSCP value of 1. The second marking sets the traffic in classes AF31 to AF33 to an IP DSCP of 3.

```
Switch(config)# policy-map Example
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set ip dscp 1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class AF31-AF33
Switch(config-pmap-c)# set ip dscp 3
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# service-policy input Example
Switch(config-if)# exit
```

### Configuring Policing

Policing is used to enforce a traffic-metering profile. A policer meters a particular traffic flow and 
determines if a packet in the given flow conforms to the specified rate. You use the `police` policy-map 
class configuration command to configure individual policers to define the committed rate limitations, 
committed burst size limitations of the traffic, and the action to take for a class of traffic.

The switch supports 1-rate policing with a 2-color marker, or 2-rate policing with a 3-color marker. 
Mapped packets can be sent without modification, dropped, or marked to the options specified by the `set` 
command. Note that traffic rates are configured in bits per second and burst size is entered in bytes.

Follow these guidelines when configuring policing.

- Hierarchical policing is not supported.
- You can configure policing for any number of classes on any one of the three levels of the 
policy-map hierarchy. If you configure marking on one level, you can configure policing without 
marking (transmit, drop) on another level.

### Configuring a Policy Map with 1-Rate, 2-Color Policing

Beginning in privileged EXEC mode, follow these steps to create a 1-rate, 2 color input policy map with 
individual policing:

<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>class <code>class-map-name</code></td>
<td>Enter a class-map name or <code>class-default</code> to match all unclassified packets, and enter policy-map class configuration mode.</td>
</tr>
<tr>
<td></td>
<td>class-default</td>
<td>If you enter a class-map name, you must have already created the class map by using the class-map global configuration command.</td>
</tr>
<tr>
<td>Step 3</td>
<td>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>
</tbody>
</table>
## Configuring QoS

### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>police</code>*rate-bps</td>
<td>Configure a traffic policer based on the traffic rate or committed information rate (CIR). By default, no policer is defined.</td>
</tr>
</tbody>
</table>
| `cir`*cir-bps `[burst-bytes] [bc-burst-bytes]]` | - For `rate-bps`, specify average traffic rate in bits per second (b/s). The range is 64000 to 1000000000.  
- For `cir cir-bps`, specify a committed information rate (CIR) in bits per second (b/s). The range is 64000 to 1000000000.  
- For `burst-bytes` (optional), specify the normal burst size in bytes. The range is 8000 to 16000000.  
- For `bc-burst-bytes` (optional), specify the conformed burst (bc) or the number of acceptable burst bytes. The range is 8000 to 16000000.  
- For `cir percent` percent, specify the rate as a percentage of the bandwidth assigned to the class. The range is 1 to 100 percent.  
- For `burst-ms` (optional), enter the conform burst size in milliseconds. The range is 1 to 2000. The default is 250 ms.  
- For `bc-burst-ms` (optional), specify the conformed burst (bc) in milliseconds. The range is 1 to 2000. |

### Note

If you are configuring a single action for conformed and exceeded packets, you can specify them in the same line as the `police` command. If configuring multiple actions, press ENTER after the `police` command, and enter policy-map class police configuration mode (config-pmap-c-police) mode to specify the actions to take.
### Step 5


(Optional) Enter the action to be taken on packets that conform to the CIR.

- **drop**—drop the packet.
- **set-cos-transmit cos_value**—set the CoS value to a new value, and send the packet. The range is 0 to 7.
- **set-discard-class-transmit discard_value**—set the discard value to a new value, and send the packet. The range is 0 to 7.
- **set-dscp-transmit dscp_value**—set the IP DSCP value to a new value, and send the packet. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value or use the question mark (?) to see a list of available values.
- **set-mpls-exp-imposition-transmit new-exp**—enter the new MPLS experimental value to be set at tag imposition, and send the packet. The range is 0 to 7.
- **set-mpls-exp-topmost-transmit new-exp**—enter the new MPLS experimental value for the outermost or topmost label, and send the packet. The range is 0 to 7.
- **set-prec-transmit value**—set the IP precedence value to a new value, and send the packet. The range is 0 to 7.
- **set-qos-transmit value**—set the QoS group number to a new value, and send the packet. The range is 0 to 99.
- **transmit**—send the packet without altering it. This is the default.

**Note** If you are configuring a single action for conformed and exceeded packets, you can specify them in the same line. If configuring multiple actions, press ENTER after the **conform-action** command.
Configuring QoS

After you create the policy map, attach it to an interface or an EFP. See the “Attaching a Service Policy to an Interface or EFP” section on page 27-71.

This example shows how to create a traffic classification with a CoS value of 4, create a policy map, and attach it to an ingress port. The average traffic rate is limited to 10000000 b/s with a burst size of 10000 bytes:

```
Switch(config)# class-map video-class
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map video-policy
Switch(config-pmap)# class video-class
Switch(config-pmap-c)# police 10000000 10000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy input video-policy
Switch(config-if)# exit
```
This example shows how to create policy map with a conform action of set dscp and a default exceed action, and attach it to an EFP.

```plaintext
Switch(config)# class-map in-class-1
Switch(config-cmap)# match dscp 14
Switch(config-cmap)# exit
Switch(config)# policy-map in-policy
Switch(config-pmap)# class in-class-1
Switch(config-pmap-c)# police 23000 8000 conform-action set-dscp-transmit 33 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-if)# interface gigabitethernet0/1
Switch(config-if)# service instance 1 Ethernet
Switch(config-if-srv)# service-policy input in-policy
Switch(config-if-srv)# exit
```

This example shows how to use policy-map class police configuration mode to set multiple conform actions and an exceed action. The policy map sets a committed information rate of 23000 bits per second (b/s) and a conform burst size of 10000 bytes. The policy map includes multiple conform actions (for DSCP and for Layer 2 CoS) and an exceed action.

```plaintext
Switch(config)# class-map cos-set-1
Switch(config-cmap)# match cos 3
Switch(config-cmap)# exit
Switch(config)# policy-map map1
Switch(config-pmap)# class cos-set-1
Switch(config-pmap-c)# police cir 23000 bc 10000
Switch(config-pmap-c-police)# conform-action set-dscp-transmit 48
Switch(config-pmap-c-police)# conform-action set-cos-transmit 5
Switch(config-pmap-c-police)# exceed-action drop
Switch(config-pmap-c-police)# exit
Switch(config-pmap)# exit
Switch(config-if)# interface gigabitethernet0/1
Switch(config-if)# service-policy input map1
Switch(config-if)# exit
```

### Configuring a Policy Map with 2-Rate, 3-Color Policing

A 2-rate, 3-color policer uses both the committed information rate (CIR) and the peak information rate (PIR) and includes three profiles (colors) for packets that conform, exceed, or violate the specified rates. You can configure actions to take on each of these profiles.

Beginning in privileged EXEC mode, follow these steps to create an input policy map with individual 2-rate, 3-color policing:

<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 class (\text{class-map-name} \mid \text{class-default})</td>
<td>Enter a class-map name or class-default to match all unclassified packets, and enter policy-map class configuration mode. If you enter a class-map name, you must have already created the class map by using the class-map global configuration command.</td>
</tr>
<tr>
<td>Step 3 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 class maps are defined.</td>
</tr>
</tbody>
</table>
### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>police</strong> {rate-bps</td>
<td>cir {cir-bps [burst-bytes] [bc burst-bytes]</td>
</tr>
<tr>
<td>• For <strong>rate-bps</strong>, specify average traffic rate in bits per second (b/s). The range is 64000 to 10000000000.</td>
<td></td>
</tr>
<tr>
<td>• For <strong>cir cir-bps</strong>, specify a committed information rate (CIR) in bits per second (b/s). The range is 64000 to 10000000000.</td>
<td></td>
</tr>
<tr>
<td>• For <strong>burst-bytes</strong> (optional), specify the normal burst size in bytes. The range is 8000 to 16000000.</td>
<td></td>
</tr>
<tr>
<td>• For <strong>bc burst-bytes</strong> (optional), specify the conformed burst (bc) or the number of acceptable burst bytes. The range is 8000 to 16000000.</td>
<td></td>
</tr>
<tr>
<td>• For <strong>cir percent percent</strong>, specify the CIR as a percentage of the bandwidth assigned to the class. The range is from 1 to 100 percent.</td>
<td></td>
</tr>
<tr>
<td>• For <strong>burst-ms</strong> (optional), enter the conform burst size in milliseconds. The range is 1 to 2000.</td>
<td></td>
</tr>
<tr>
<td>• For <strong>bc burst-ms</strong> (optional), specify the conformed burst (bc) in ms. The range is 1 to 2000.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) For <strong>pir pir-bps</strong>, specify the peak information rate (PIR) for the policy. The range is 64000 to 10000000000. If you do not enter a <strong>pir pir-bps</strong>, the policer is configured as a 1-rate, 2-color policer.</td>
<td></td>
</tr>
<tr>
<td>• For <strong>be peak-burst</strong> (optional), specify the peak burst size in bytes. The range is 8000 to 16000000 bytes. The default is internally calculated based on the user configuration. You cannot configure this option unless you have entered the <strong>pir</strong> keyword.</td>
<td></td>
</tr>
<tr>
<td>• For <strong>pir percent percent</strong>, specify the PIR as a percentage of the bandwidth assigned to the class. The range is 1 to 100 percent. if you enter cir percent, you must enter pir in percent.</td>
<td></td>
</tr>
<tr>
<td>• For <strong>be burst-ms</strong> (optional), specify the peak burst in ms. The range is 1 to 2000.</td>
<td></td>
</tr>
</tbody>
</table>

**Note** If you are configuring a single action for conformed and exceeded packets, you can specify them in the same line as the **police** command. If configuring multiple actions, press ENTER after the **police** command, and enter policy-map class police configuration mode (config-pmap-c-police) mode to specify the actions to take.
Chapter 27  Configuring Quality of Service (QoS)

**Step 5**

```bash


```

(Optional) Enter the action to be taken on packets, depending on whether or not they conform to the CIR and PIR.

- (Optional) For **conform-action**, specify the action to perform on packets that conform to the CIR and PIR. The default is **transmit**.
- (Optional) For **exceed-action**, specify the action to perform on packets that conform to the PIR but not the CIR. The default is **drop**.
- (Optional) For **violate-action**, specify the action to perform on packets that exceed the PIR. This keyword is only visible when you have entered `pir` after the `police` command. The default is **drop**.

Specify one of these actions to perform on the packets:

- **drop**—drop the packet.
- **set-cos-transmit cos_value**—set the CoS value to a new value, and send the packet. The range is 0 to 7.
- **set-discard-class-transmit discard_value**—set the discard value to a new value, and send the packet. The range is 0 to 7.
- **set-dscp-transmit dscp_value**—set the IP DSCP value to a new value, and send the packet. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value.
- **set-mpls-exp-imposition-transmit new-exp**—enter the new MPLS experimental value to be set at tag imposition, and send the packet. The range is 0 to 7.
- **set-mpls-exp-topmost-transmit new-exp**—enter the new MPLS experimental value for the outermost or topmost label, and send the packet. The range is 0 to 7.
- **set-prec-transmit value**—set the IP precedence value to a new value, and send the packet. The range is 0 to 7.
- **set-qos-transmit value**—set the QoS group number to a new value, and send the packet. The range is 0 to 99.
- **transmit**—send the packet without altering it.

**Note** If the conform action is set to **drop**, the exceed and violate actions are automatically set to **drop**. If the exceed action is set to **drop**, the violate action is automatically set to **drop**.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>conform-action</code></td>
<td>(Optional) Enter the action to be taken on packets, depending on whether or not they conform to the CIR and PIR.</td>
</tr>
<tr>
<td><code>set-cos-transmit cos_value</code></td>
<td>(Optional) Set the CoS value to a new value, and send the packet. The range is 0 to 7.</td>
</tr>
<tr>
<td><code>set-discard-class-transmit discard_value</code></td>
<td>(Optional) Set the discard value to a new value, and send the packet. The range is 0 to 7.</td>
</tr>
<tr>
<td><code>set-dscp-transmit dscp_value</code></td>
<td>(Optional) Set the IP DSCP value to a new value, and send the packet. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value.</td>
</tr>
<tr>
<td><code>set-mpls-exp-imposition-transmit new-exp</code></td>
<td>(Optional) Enter the new MPLS experimental value to be set at tag imposition, and send the packet. The range is 0 to 7.</td>
</tr>
<tr>
<td><code>set-mpls-exp-topmost-transmit new-exp</code></td>
<td>(Optional) Enter the new MPLS experimental value for the outermost or topmost label, and send the packet. The range is 0 to 7.</td>
</tr>
<tr>
<td><code>set-prec-transmit value</code></td>
<td>(Optional) Set the IP precedence value to a new value, and send the packet. The range is 0 to 7.</td>
</tr>
<tr>
<td><code>set-qos-transmit value</code></td>
<td>(Optional) Set the QoS group number to a new value, and send the packet. The range is 0 to 99.</td>
</tr>
<tr>
<td><code>transmit</code></td>
<td>(Optional) Send the packet without altering it.</td>
</tr>
</tbody>
</table>

**Step 6**

```
end
```

Return to privileged EXEC mode.

**Step 7**

```
show policy-map [policy-map-name]
```

Verify your entries.

**Step 8**

```
copy running-config startup-config
```

(Optional) Save your entries in the configuration file.
After you create the policy map, attach it to an interface or an EFP. See the “Attaching a Service Policy to an Interface or EFP” section on page 27-71.

Use the no form of the appropriate command to delete an existing policy map, class map, or policer.

This example shows how to configure 2-rate, 3-color policing using policy-map configuration mode.

```
Switch(config)# class-map cos-4
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map in-policy
Switch(config-pmap)# class cos-4
Switch(config-pmap-c)# police cir 5000000 pir 8000000 conform-action transmit exceed-action set-dscp-transmit 24 violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy input in-policy
Switch(config-if)# exit
```

This example shows how to create the same configuration using policy-map class police configuration mode.

```
Switch(config)# class-map cos-4
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map in-policy
Switch(config-pmap)# class cos-4
Switch(config-pmap-c)# police cir 5000000 pir 8000000
Switch(config-pmap-c-police)# conform-action transmit
Switch(config-pmap-c-police)# exceed-action set-dscp-transmit 24
Switch(config-pmap-c-police)# violate-action drop
Switch(config-pmap-c-police)# end
```

### Configuring Output Policy Maps

- Configuring Output Class Maps, page 27-48
- Configuring Class-Based-Weighted Fair Queuing, page 27-51
- Configuring Class-Based Shaping, page 27-54
- Configuring Port Shaping, page 27-55
- Configuring Class-Based Priority Queuing, page 27-60
- Configuring Policing, page 27-57
- Configuring Marking, page 27-56
- Configuring Weighted Tail Drop, page 27-62

### Configuring Output Class Maps

You use the class-map global configuration command to name and to isolate a specific traffic flow (or class) from all other traffic. A class map defines the criteria to use to match against a specific traffic flow to further classify it. Match statements can include criteria such as an inner or outer CoS value, DSCP value, IP precedence values, QoS group values, discard class, MPLS experimental labels, or inner or outer VLAN IDs. You define match criterion with one or more match statements entered in the class-map configuration mode.
In an output policy, the match criteria acts on the packet on the wire after any VLAN rewrite mapping operations on egress.

Beginning in privileged EXEC mode, follow these steps to create a class map and to define the match criterion to classify traffic:

<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>class-map [match-all</td>
<td>match-any] class-map-name</td>
</tr>
</tbody>
</table>

**Note**

The **match-all** keyword is supported only for outer VLAN and inner VLAN, or outer CoS and inner CoS matches for QinQ packets. The **match-all** keyword is rejected for all other mutually exclusive match criteria.

- (Optional) Use the **match-all** keyword to perform a logical AND of all matching statements under this class map. All match criteria in the class map must be matched.
- (Optional) Use the **match-any** keyword to perform a logical OR of all matching statements under this class map. One or more match criteria must be matched.
- For class-map-name, specify the name of the class map.

If no matching statements are specified, the default is **match-all**.

**Note**

A **match-all** class map cannot have more than one classification criterion (match statement) except to match outer and inner 802.1Q VLAN tag of QinQ packets using **match vlan** and **match vlan inner** or **match cos** and **match cos inner**.
Configuring QoS

Step 3

**Command**

match {cos-cos-list | cos inner cos-list | discard-class-value | ip dscp dscp-list | ip precedence ip-precedence-list | mpls experimental topmost value | qos-group value | vlan-vlan-list | vlan inner vlan-list}

**Purpose**

Define the match criterion to classify traffic. By default, no match criterion is defined. Only one match type per class map is supported, and only one ACL per class map is supported.

- Enter `cos-cos-list` to match a packet based on the outer VLAN tag or the service-provider CoS value. You can specify up to four Layer 2 CoS values to match against the packet. Separate each value with a space. The range is 0 to 7.

- Enter `cos inner cos-list` to match a packet based on the inner CoS value. For packets with less than two tags, this command has no effect. You can specify up to four Layer 2 CoS values to match against the packet. Separate each value with a space. The range is 0 to 7.

- Enter `discard-class-value` to match a packet based on the drop precedence for a packet during congestion management. The range is 0 to 7. Matching discard class is supported only in output policy maps.

- For `ip dscp dscp-list`, enter a list of up to eight IPv4 DSCP values to match against incoming packets. Separate each value with a space. You can enter multiple `dscp-list` lines to match more than eight DSCP values. The numerical range is 0 to 63. You can also configure DSCP values in other forms (af numbers, cs numbers, `default`, or `ef`).

- For `ip precedence ip-precedence-list`, enter a list of up to four IPv4 precedence values to match against incoming packets. Separate each value with a space. You can enter multiple `ip-precedence-list` lines to match more than four precedence values. The range is 0 to 7.

- For `mpls experimental topmost value`, enter a list of up to eight MPLS experimental labels. You can enter multiple lines to match more than eight MPLS experimental values. This keyword matches only valid MPLS packets. Separate each value with a space. The range is 0 to 7.

- For `qos-group value`, specify the QoS group number. The range is 0 to 99. Matching of QoS groups is supported only in output policy maps.

- Enter `vlan vlan-id` to match a packet based on the outermost, service-provider VLAN ID (S-VLAN). For untagged packets, this matches the default VLAN associated with the packets from the port or EFP. You can enter a single VLAN ID or a range of VLANs separated by a hyphen. The range is from 1 to 4095.

- Enter `vlan inner vlan-id` to match a packet based on the C-VLAN, the inner customer VLAN ID of an 802.1Q tunnel. For packets with less than 2 tags, the command has no effect. You can specify a single VLAN identified by a VLAN number or a range of VLANs separated by a hyphen. The range is 1 to 4094.

Step 4

**end**

Return to privileged EXEC mode.

Step 5

**show class-map**

Verify your entries.

Step 6

**copy running-config startup-config**

(Optional) Save your entries in the configuration file.

Use the no form of the appropriate command to delete an existing class map or remove a match criterion.
This example shows how to create a class map called `class2`, which matches traffic with DSCP values of 10, 11, and 12.

```config
Switch(config)# class-map match-any 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 traffic with IP-precedence values of 5, 6, and 7:

```config
Switch(config)# class-map match-any class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# exit
```

This example shows how to create a class-map called `parent-class`, which matches traffic with VLAN IDs in the range from 30 to 40.

```config
Switch(config)# class-map match-any parent-class
Switch(config-cmap)# match vlan 30-40
Switch(config-cmap)# exit
```

### Configuring Class-Based-Weighted Fair Queuing

You use the `bandwidth` policy-map class configuration command to configure class-based weighted fair queuing (CBWFQ). CBWFQ sets the explicit minimum guaranteed rate (CIR) of a class by reserving the configured bandwidth for that class.

Follow these guidelines:

- You can configure CBWFQ at the class level and at the VLAN level.
- The total of the minimum bandwidth guaranteed for each queue of the policy cannot exceed the total speed of the parent.
- You cannot configure bandwidth as an absolute rate or a percentage of total bandwidth when strict priority is configured for another class in the output policy.
- You can configure bandwidth as percentage of remaining bandwidth when strict priority is configured for another class in the output policy map.
- You cannot configure bandwidth and priority or bandwidth and traffic shaping for the same class in an output policy map.

Beginning in privileged EXEC mode, follow these steps to use CBWFQ to control bandwidth allocated to a traffic class by specifying a minimum bandwidth as a bit rate or a percentage:

<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>policy-map policy-map-name</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>class {class-map-name</td>
</tr>
</tbody>
</table>
Configuring QoS

After you create the policy map, attach it to an interface or an EFP. See the “Attaching a Service Policy to an Interface or EFP” section on page 27-71. Use the no form of the appropriate command to delete an existing policy map, class map, or bandwidth configuration.

**Note**
If you enter the no policy-map configuration command or the no policy-map policy-map-name global configuration command to delete a policy map that is attached to an interface, a warning message appears that lists any interfaces from which the policy map is being detached. The policy map is then detached and deleted. For example:

Warning: Detaching Policy test1 from Interface GigabitEthernet0/1

This example shows how to allocate 25 percent of the total available bandwidth to the traffic class defined by the class map:

```
Switch(config)# policy-map gold_policy
Switch(config-pmap)# class out_class-1
Switch(config-pmap-c)# bandwidth percent 25
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output gold_policy
Switch(config-if)# exit
```

**Note**
When you configure CIR bandwidth for a class as an absolute rate or percentage of the total bandwidth, any excess bandwidth remaining after servicing the CIR of all the classes in the policy map is divided among the classes in the same proportion as the CIR rates. If the CIR rate of a class is configured as 0, that class is not eligible for any excess bandwidth and, as a result, receives no bandwidth.
This example shows how to set the precedence of output queues by setting bandwidth in kilobits per second. The classes \textit{outclass1}, \textit{outclass2}, and \textit{outclass3} and \textbf{class-default} get a minimum of 40000, 20000, 10000, and 10000 kb/s. Any excess bandwidth is divided among the classes in the same proportion as the CIR rate.

\begin{verbatim}
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth 40000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth 20000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth 10000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth 10000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
\end{verbatim}

This example shows how to allocate the excess bandwidth among queues by configuring bandwidth for a traffic class as a percentage of remaining bandwidth. The class \textit{outclass1} is given priority queue treatment. The other classes are configured to get percentages of the excess bandwidth if any remains after servicing the priority queue: \textit{outclass2} is configured to get 50 percent, \textit{outclass3} to get 20 percent, and the class \textbf{class-default} to get the remaining 30 percent.

\begin{verbatim}
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
\end{verbatim}

This example shows how to match VLAN and CoS in the same policy. When you attach the service policy \textit{vlan} to an interface, packets with the outer VLAN of 2 and an outer CoS of 2 are included in class map \textit{phb}.

\begin{verbatim}
Switch(config)# class-map vlan
Switch(config-cmap)# match vlan 2
Switch(config-cmap)# exit
Switch(config)# class-map phb
Switch(config-cmap)# match cos 2
Switch(config-cmap)# exit
Switch(config)# policy-map phb
Switch(config-pmap)# class phb
Switch(config-pmap-c)# bandwidth 1000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map vlan
Switch(config-pmap)# class vlan
Switch(config-pmap-c)# bandwidth 1000
Switch(config-pmap-c)# service-policy phb
\end{verbatim}
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# service-policy vlan
Switch(config-if)# exit

Configuring Class-Based Shaping

You use the `shape average` policy-map class configuration command to configure traffic shaping. Class-based shaping sets the explicit maximum peak information rate (PIR) for the class by limiting it to the configured bandwidth. You can configure class-based shaping at the class level and at the VLAN level.

Beginning in privileged EXEC mode, follow these steps to use class-based shaping to configure the maximum permitted average rate for a class of traffic:

<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>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></td>
<td>policy-map configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>`class {class-map-name</td>
<td>class-default}`</td>
</tr>
<tr>
<td></td>
<td></td>
<td>unclassified packets, and enter policy-map class configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mode.</td>
</tr>
<tr>
<td>4</td>
<td>`shape average {target bps</td>
<td>percent value}`</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For <code>target bps</code>, specify the average bit rate in bits per second.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The range is from 1000 to 10000000000 (10 Gigabits).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter <code>percent value</code> to set the percentage of interface</td>
</tr>
<tr>
<td></td>
<td></td>
<td>bandwidth for peak information rate. The range is 0 to 100 percent.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The percentage is calculated based on the peak information rate (PIR)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>of the parent class. If there is no configured PIR at any level, this</td>
</tr>
<tr>
<td></td>
<td></td>
<td>is the percentage of the interface speed. Setting the percent to 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>disables shaping.</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 policy-map [policy-map-name [class class-map-name]]</code></td>
<td>Verify your entries.</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>

After you create the policy map, attach it to an interface or an EFP. See the “Attaching a Service Policy to an Interface or EFP” section on page 27-71. Use the **no** form of the appropriate command to delete an existing policy map or class map or to delete a class-based shaping configuration.

This example shows how to configure traffic shaping for outgoing traffic on a Gigabit Ethernet port so that `outclass1`, `outclass2`, and `outclass3` get a maximum of 50, 20, and 10 Mb/s of the available port bandwidth.

Switch(config)# `policy-map out-policy`
Switch(config-pmap)# `class classout1`
Switch(config-pmap-c)# `shape average 50000000`
Switch(config-pmap-c)# `exit`
Switch(config-pmap)# `class classout2`
Switch(config-pmap-c)# `shape average 20000000`
Switch(config-pmap-c)# `exit`
### Configuring Port Shaping

Port shaping is applied to all traffic leaving an interface. It uses a policy map with only class default when the maximum bandwidth for the port is specified by using the `shape average` command. A child policy can be attached to the class-default in a hierarchical policy map format to specify class-based and VLAN-based actions.

Beginning in privileged EXEC mode, follow these steps to use port shaping to configure the maximum permitted average rate for a class of traffic:

<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>policy-map policy-map-name</code></td>
<td>Create a hierarchical policy map by entering the hierarchical policy map name, and enter policy-map configuration mode for the parent policy.</td>
</tr>
<tr>
<td>3</td>
<td><code>class class-default</code></td>
<td>Enter a policy-map class configuration mode for the default class.</td>
</tr>
<tr>
<td>4</td>
<td>`shape average {target bps</td>
<td>percent value}`</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For <code>target bps</code>, specify the average bit rate in bits per second. The range is from 1000 to 10000000000 (10 Gigabits).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter <code>percent value</code> to set the percentage of interface bandwidth for peak information rate. The range is 0 to 100 percent. The percentage is based on the port operational link speed. Setting the percent to 0 disables shaping.</td>
</tr>
<tr>
<td>5</td>
<td><code>service-policy policy-map-name</code></td>
<td>Specify the child policy-map to be used in the hierarchical policy map if required.</td>
</tr>
<tr>
<td>6</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>7</td>
<td><code>show policy-map [policy-map-name [class class-map-name]]</code></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>8</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

After you create the policy map, attach it to an interface or an EFP. See the “Attaching a Service Policy to an Interface or EFP” section on page 27-71.

Use the `no` form of the appropriate command to delete an existing hierarchical policy map, to delete a port shaping configuration, or to remove the policy map from the hierarchical policy map.

This example shows how to configure port shaping by configuring a hierarchical policy map that shapes a port to 90 Mb/s, allocated according to the `out-policy` policy map configured in the previous example.

```
Switch(config)# policy-map out-policy-parent
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 90000000
Switch(config-pmap-c)# service-policy out-policy
Switch(config-pmap-c)# exit
```
Configuring QoS

Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output out-policy-parent
Switch(config-if)# exit

Configuring Marking

Use the set policy-map class configuration command to set or modify the attributes for traffic belonging to a specific class.

Follow these guidelines when configuring class-based marking:

- Hierarchical marking is not supported.
- You can only configure egress marking for classes on the third level of the policy map hierarchy.

In the privileged EXEC mode, perform these steps to create an output policy map that marks traffic.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>policy-map policy-map-name</td>
</tr>
<tr>
<td>Step 3</td>
<td>class {class-map-name</td>
</tr>
</tbody>
</table>
| Step 4 | set {cos cos_value | discard-class value | [ip] dscp dscp_value | [ip] precedence precedence_value | mpls experimental {topmost} experimental _value} | Mark traffic by setting a new value in the packet, specifying a table map, or specifying a QoS group.
- For cos cos_value, enter a new CoS value to be assigned to the classified traffic. The range is 0 to 7.
- For [ip] dscp new-dscp, enter a new DSCP value to be assigned to the classified traffic. The range is 0 to 63 or valid af numbers, cs numbers, default, or ef.
- For [ip].precedence new-precedence, enter a new IP precedence value to be assigned to the classified traffic, 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).

**Note** A class can have either DSCP or precedence marking. If one of these is already configured in a class and you configure the other keyword, the newer command overwrites the previous command. If the value configured for a set ip precedence class in an earlier class in a policy overlaps the value configured for a set ip dscp class in a later class, the earlier configuration is always matched.

- For mpls experimental topmost exp-number, enter the new MPLS experimental value for the outermost or topmost label. This keyword marks all the valid MPLS packets. The range is 0 to 7.

If the policy is already attached to an interface, you must exit the policy-map class configuration mode before the modification is applied.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
</tbody>
</table>
Chapter 27  Configuring Quality of Service (QoS)

Configuring QoS

After you create the input policy map, attach it to a target. See the “Attaching a Service Policy to an Interface or EFP” section on page 27-71. Use the no form of the appropriate command to delete a policy map or remove an assigned CoS, DSCP, MPLS, or precedence value.

This example uses a policy map to re-mark a packet. The first marking (the set command) applies to the QoS default class map that matches all the traffic not matched by class AF31-AF33 and sets all the traffic to an IP DSCP value of 1. The second marking sets the traffic in classes AF31 to AF33 to an IP DSCP of 3.

Switch(config)# policy-map Example
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set ip dscp 1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class AF31-AF33
Switch(config-pmap-c)# set ip dscp 3
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# service-policy input Example
Switch(config-if)# exit

Configuring Policing

Policing is used to enforce a traffic-metering profile. A policer meters a particular traffic flow and determines if a packet in the given flow conforms to the specified rate. Use the police policy map class configuration command to configure individual policers to define the committed rate limitations, committed burst size limitations of the traffic, and the action to take for a class of traffic.

The switch supports 1-rate policing with a 2-color marker. Mapped packets can be sent without modification, dropped, or marked to the options specified by the set command. Note that traffic rates are configured in bits per second and burst size is entered in bytes.

Follow these guidelines when configuring policing:

- Hierarchical policing is not supported.

Configuring a Policy Map with 1-Rate, 2-Color Policing

In the privileged EXEC mode, perform these steps to create a 1-rate, 2 color output policy map with individual policing.

<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 the 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>class {class-map-name</td>
<td>class-default}</td>
</tr>
</tbody>
</table>
### Chapter 27      Configuring Quality of Service (QoS)

#### Configuring QoS

**Step 3**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `policy-map policy-map-name` | Create a policy map by entering the policy map name, and enter policy-map configuration mode. By default, no policy maps are defined.

**Step 4**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`police {rate-bps</td>
<td>cir {cir-bps [burst-bytes] [bc-burst-bytes]}</td>
</tr>
<tr>
<td></td>
<td>- For <code>rate-bps</code>, specify average traffic rate in bits per second (b/s). The range is 64000 to 10000000000.</td>
</tr>
<tr>
<td></td>
<td>- For <code>cir cir-bps</code>, specify a committed information rate (CIR) in bits per second (b/s). The range is 64000 to 10000000000.</td>
</tr>
<tr>
<td></td>
<td>- For <code>burst-bytes</code> (optional), specify the normal burst size in bytes. The range is 8000 to 16000000.</td>
</tr>
<tr>
<td></td>
<td>- For <code>bc-burst-bytes</code> (optional), specify the conformed burst (bc) or the number of acceptable burst bytes. The range is 8000 to 16000000.</td>
</tr>
<tr>
<td></td>
<td>- For <code>cir percent percent</code>, specify the rate as a percentage of the bandwidth assigned to the class. The range is 1 to 100 percent.</td>
</tr>
<tr>
<td></td>
<td>- For <code>burst-ms</code> (optional), enter the conform burst size in milliseconds. The range is 1 to 2000. The default is 250 ms.</td>
</tr>
<tr>
<td></td>
<td>- For <code>bc-burst-ms</code> (optional), specify the conformed burst (bc) in milliseconds. The range is 1 to 2000.</td>
</tr>
</tbody>
</table>

**Note**

If you are configuring a single action for conformed and exceeded packets, you can specify them in the same line as the `police` command. If configuring multiple actions, press ENTER after the `police` command, and enter policy-map class police configuration mode (config-pmap-c-police) mode to specify the actions to take.

**Step 5**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`conform-action {drop</td>
<td>set-cos-transmit cos_value</td>
</tr>
<tr>
<td></td>
<td>- <code>drop</code>—Drop the packet.</td>
</tr>
<tr>
<td></td>
<td>- <code>set-cos-transmit cos_value</code>—Set the CoS value to a new value and send the packet. The range is 0 to 7.</td>
</tr>
<tr>
<td></td>
<td>- <code>set-dscp-transmit dscp_value</code>—Set the IP DSCP value to a new value and send the packet. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value or use the question mark (?) to see a list of available values.</td>
</tr>
<tr>
<td></td>
<td>- <code>set-mpls-exp-topmost-transmit new-exp</code>—Enter the new MPLS experimental value for the outermost or topmost label, and send the packet. The range is 0 to 7.</td>
</tr>
<tr>
<td></td>
<td>- <code>set-prec-transmit value</code>—Set the IP precedence value to a new value and send the packet. The range is 0 to 7.</td>
</tr>
<tr>
<td></td>
<td>- <code>transmit</code>—Send the packet without altering it. This is the default.</td>
</tr>
</tbody>
</table>

**Note**

If you are configuring a single action for conforming and exceeding packets, you can specify them in the same line. If configuring multiple actions, press ENTER after the `conform-action` command.
### Step 6

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>exceed-action { drop</td>
<td>set-cos-transmit cos_value</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>

**Note** If you explicitly configure **exceed-action drop** as keywords in the command, you must enter the policy-map class police configuration mode and enter the **no exceed-action drop** command to remove the previously configured exceed action before you can enter the new exceed action.

---

### Step 7

**end**

Return to the privileged EXEC mode.

### Step 8

**show policy-map [policy-map-name [class class-map-name]]**

Verify your entries.

### Step 9

**copy running-config startup-config**

(Optional) Save your entries in the configuration file.

---

After you create the policy map, attach it to an interface or an EFP. See the “Attaching a Service Policy to an Interface or EFP” section on page 27-71.

This example shows how to create a traffic classification with a CoS value of 4, create a policy map, and attach it to an egress port. The average traffic rate is limited to 10000000 b/s with a burst size of 10000 bytes.

```
Switch(config)# class-map video-class
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map video-policy
Switch(config-pmap)# class video-class
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police cir 10000000 bc 10000
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output video-policy
Switch(config-if)# exit
```

This example shows how to create a policy map with a conform action of **set dscp** and a default exceed action, and attach it to an EFP.

```
Switch(config)# class-map in-class-1
Switch(config-cmap)# match dscp 14
Switch(config-cmap)# exit
Switch(config)# policy-map out-policy
Switch(config-pmap)# class out-class-1
```

---

Cisco ME 3800X and ME 3600X Switch Software Configuration Guide

OL-23400-02

27-59
Configuring QoS

Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police cir 230000 bc 8000 conform-action set-dscp-transmit 33
              exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# service-policy output out-policy
Switch (config-if-srv)# exit

This example shows how to configure port shaping when EFP policies are present, by configuring a
hierarchical policy map that shapes a port to 50 percent, allocated according to the *out-policy* policy map
configured in the previous example.

Switch(config)# policy-map port-policy
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average percent 50
Switch(config-pmap-c)# service-policy out-policy
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output out-policy-parent
Switch(config-if)# exit

This example shows how to use the policy-map class police configuration mode to set multiple conform
actions and an exceed action. The policy map sets a committed information rate of 23000 bits per second
(b/s) and a conform burst size of 10000 bytes. The policy map includes multiple conform actions (for
DSCP and Layer 2 CoS) and an exceed action.

Switch(config)# class-map cos-set-1
Switch(config-cmap)# match cos 3
Switch(config-cmap)# exit
Switch(config)# policy-map map1
Switch(config-pmap)# class cos-set-1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police cir 23000 bc 10000
Switch(config-pmap-c-police)# conform-action set-dscp-transmit 48
Switch(config-pmap-c-police)# conform-action set-cos-transmit 5
Switch(config-pmap-c-police)# exceed-action drop
Switch(config-pmap-c-police)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output map1
Switch(config-if)# exit

### Configuring Class-Based Priority Queuing

You can use the *priority* policy-map class configuration command to ensure that a particular class of
traffic is given preferential treatment. Strict priority queuing provides low-latency service to the class.

- When priority is configured in an output policy map without the police command, you can only
  configure the other queues for sharing by using the bandwidth remaining percent policy-map
  command to allocate excess bandwidth.
- You can apply priority at the class level and to the VLAN level.
- You can associate the priority command with a single class at the class level and a single class at the
  VLAN level.
Beginning in privileged EXEC mode, follow these steps to configure a strict priority queue:

<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 class-map class-map-name</td>
<td>Create classes for three egress queues. Enter match conditions classification for each class.</td>
</tr>
<tr>
<td>Step 3 policy-map policy-map-name</td>
<td>Create a policy map by entering the policy map name, and enter policy-map configuration mode.</td>
</tr>
<tr>
<td>Step 4 class-class-map-name</td>
<td>Enter the name of the priority class (created by using the class-map global configuration command), and enter policy-map class configuration mode for the priority class.</td>
</tr>
<tr>
<td>Step 5 priority</td>
<td>Set the strict scheduling priority for this class.</td>
</tr>
<tr>
<td>Note</td>
<td>Only one unique class map in an attached policy map can be associated with a priority command. You cannot configure priority along with any other queuing action (bandwidth or shape average).</td>
</tr>
<tr>
<td>Step 6 exit</td>
<td>Exit policy-map class configuration mode for the priority class.</td>
</tr>
<tr>
<td>Step 7 class class-map-name</td>
<td>Enter the name of a nonpriority class, and enter policy-map class configuration mode for that class.</td>
</tr>
<tr>
<td>Step 8 bandwidth remaining percent value</td>
<td>Set output bandwidth limits for the policy-map class as a percentage of the remaining bandwidth. The range is 0 to 100 percent.</td>
</tr>
<tr>
<td>Step 9 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 10 show policy-map</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 11 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

After you have created an output policy map, you attach it to an egress port or EFP. See the “Attaching a Service Policy to an Interface or EFP” section on page 27-71.

Use the no form of the appropriate command to delete an existing policy map or class map or to cancel strict priority queuing for the priority class or the bandwidth setting for the other classes.

This example shows how to configure the class `out-class1` as a strict priority queue so that all packets in that class are sent before any other class of traffic. Other traffic queues are configured so that `out-class-2` gets 50 percent of the remaining bandwidth and `out-class3` gets 20 percent of the remaining bandwidth. The class `class-default` receives the remaining 30 percent with no guarantees.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit
```
Configuring Weighted Tail Drop

Weighted tail drop (WTD) adjusts the queue size associated with a traffic class in terms of time and bytes. You configure WTD by using the `queue-limit` policy-map class configuration command. The queue-limit command is allowed only after you have configured a scheduling action (bandwidth, shape average, or priority).

Beginning in privileged EXEC mode, follow these steps to use WTD to adjust the queue size for a traffic class:

<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>policy-map <code>policy-map-name</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>class-`{class-map-name</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>bandwidth `{rate</td>
</tr>
<tr>
<td></td>
<td>or shape average `{target bps</td>
</tr>
<tr>
<td></td>
<td>or priority</td>
</tr>
</tbody>
</table>
Chapter 27  Configuring Quality of Service (QoS)

Configuring QoS

After you have created an output policy map, you attach it to an egress port. See the “Attaching a Service Policy to an Interface or EFP” section on page 27-71. Use the no form of the appropriate command to delete an existing policy map or class map or to delete a WTD configuration.

**Step 5**

```
queue-limit [cos value | discard-class value | dscp value | exp value | precedence value | qos-group value] number-of-packets [packets] | limit [bytes | us]]
```

Specify the queue size for the traffic class.

- (Optional) For `cos value`, specify a CoS value. The range is from 0 to 7.
- (Optional) Enter `discard-class value` to specify the drop precedence for a packet during congestion management. The range is 0 to 7.
- (Optional) For `dscp value`, specify a DSCP value. The range is from 0 to 63.
- (Optional) For `exp value`, specify an MPLS experimental value. The range is from 0 to 7.
- (Optional) For `precedence value`, specify an IP precedence value. The range is from 0 to 7.
- (Optional) For `qos-group value`, enter a QoS group value. The range is from 0 to 99.
- (Optional) For packets,
  - For `bytes bytes`, enter the maximum threshold in bytes. The range is from 200 to 491520. The default depends on the interface speed.
    - On 10/100/1000 Mb/s interfaces, the default is 12000 (12 K) bytes.
    - On 10 Gb/s interfaces, the default is 120000 (120 K) bytes.
  - For `us microseconds`, enter the maximum threshold in microseconds. This is the default for specifying threshold. The range is from 1 to 3932. The default depends on the interface speed.
    - On 10 Mb/s interfaces, the default is 10000 us.
    - On 100 Mb/s interfaces, the default is 1000 us.
    - On 1000 Mb/s and 10 Gb/s interfaces, the default is 100 us.
  - If you do not enter `bytes bytes` or `us microseconds`, the default is `us`.

**Step 6**

```
end
```

Return to privileged EXEC mode.

**Step 7**

```
show policy-map [policy-map-name [class class-map-name]]
```

Verify your entries.

**Step 8**

```
copy running-config startup-config
```

(Optional) Save your entries in the configuration file.

---

After you have created an output policy map, you attach it to an egress port. See the “Attaching a Service Policy to an Interface or EFP” section on page 27-71. Use the no form of the appropriate command to delete an existing policy map or class map or to delete a WTD configuration.

**Note**

If the device connected to a 10/100/1000 Mb/s interface starts bursting the traffic more than the 1 Gigabit line rate because of multicast replication, you should increase the queue-limit for the policy map class applied to the interface to 48000 (48 K) bytes because the interface cannot handle the excess burst.
Chapter 27  Configuring Quality of Service (QoS)

This example shows a policy map with a specified bandwidth and queue size. Traffic that is not DSCP 30 or 10 is assigned a queue-limit of 2000 bytes. Traffic with a DSCP value of 30 is assigned a queue-limit of 1000 bytes, and traffic with a DSCP value of 10 is assigned a queue-limit of 1500 bytes. All traffic not belonging to the class traffic is classified into class-default, which is configured with 10 percent of the total available bandwidth and a large queue size of 3000 bytes.

```
Switch(config)# policy-map gold-policy
Switch(config-pmap)# class traffic
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# queue-limit bytes 2000
Switch(config-pmap-c)# queue-limit dscp 30 bytes 1000
Switch(config-pmap-c)# queue-limit dscp 10 bytes 1500
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit bytes 3000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output gold-policy
Switch(config-if)# exit
```

There can be only three unique qualified queue-limit thresholds. In this example, there are four unique thresholds, so the configuration is rejected:

```
Switch(config-pmap-c)# queue-limit 100 us
Switch(config-pmap-c)# queue-limit cos 2 200 us
Switch(config-pmap-c)# queue-limit cos 3 300 us
Switch(config-pmap-c)# queue-limit cos 4 400 us
```

In the next example, although there appear to be only three unique thresholds, in reality there are four threshold configurations, including an implied default threshold. The configuration is rejected.

```
Switch(config-pmap-c)# queue-limit cos 2 200 us
Switch(config-pmap-c)# queue-limit cos 3 300 us
Switch(config-pmap-c)# queue-limit cos 4 400 us
```

In this last example, there are only three unique thresholds and the configuration is allowed.

```
Switch(config-pmap-c)# queue-limit 100 us
Switch(config-pmap-c)# queue-limit cos 2 100 us
Switch(config-pmap-c)# queue-limit cos 3 300 us
Switch(config-pmap-c)# queue-limit cos 4 400 us
```

### Configuring Weighted Random Early Detection

This section describes the tasks involved in configuring Weighted Random Early Detection (WRED).

#### Restrictions and Usage Guidelines

- Whales supports the following commands:
  - "Outer COS (random-detect cos-based)
  - WRED based on IPv4 DSCP (random-detect dscp-based)
  - WRED based on IPv4 Precedence (random-detect precedence-based)
  - WRED based on EXP
- WRED policies is supported on below targets.
Chapter 27  Configuring Quality of Service (QoS)

Configuring QoS

– L3 Main interface
– Switchport interface
– Service instance
– Port-channel Member-link interface.

- Maximum of 2 WRED curves are supported.
- WRED configuration is supported only in egress policy-map.
- Default value for exponential-weighting-constant is 9.
- Default value for mark-probability is 10.
- Minimum-threshold and maximum-threshold can be specified in terms of packets only.
- WRED command is supported either with shape or CBWFQ command.
- WRED is supported in PHB level. Not supported in logical/physical level classes
- MQC based WRED counters are not supported.
- WRED Non-aggregate mode is not supported.
- WRED is not supported in priority queues.
- WRED is not supported based on discard class.

When a packet arrives, the following events occur:

1. The average queue size is calculated.
2. If the average is less than the minimum queue threshold, the arriving packet is queued.
3. If the average is between the minimum queue threshold for that type of traffic and the maximum threshold for the interface, the packet is either dropped or queued, depending on the packet drop probability for that type of traffic.
4. If the average queue size is greater than the maximum threshold, the packet is dropped.

See Weighted Random Early Detection (WRED), page 27-21 for more details on how WRED works.

To configure WRED on a switch, perform the tasks described in the following sections. The tasks described in the first section are required; the tasks described in the remaining sections are optional.

- Enabling WRED, page 27-65 (Required)
- Changing the WRED Parameters, page 27-66 (Optional)

Note

WTD and WRED cannot be configured under the same class of a policy map.

Enabling WRED

In the privileged EXEC mode, perform the following steps to enable WRED for a class in a policy map.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enable the 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.</td>
</tr>
<tr>
<td><strong>Step 3</strong> class-{class-map-name class-default}</td>
<td>Enter a child class map name or enter the class-default command to match all the unclassified packets, and enter the policy-map class configuration mode.</td>
</tr>
</tbody>
</table>
Chapter 27  Configuring Quality of Service (QoS)

Configuring QoS

The following example configures a policy for a class called acl10 included in a policy map called policy10:

```
Switch# configure terminal
Switch(config)# policy-map policy10
Switch(config-pmap)# class acl10
Switch(config-pmap-c)# random-detect dscp-based
Switch(config-pmap-c)# random-detect precedence 3 500 1000 10
Switch(config-pmap-c)# exit
```

Changing the WRED Parameters

To change the WRED parameters, use the following commands in the interface configuration mode, as needed.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enable global configuration mode.</td>
</tr>
<tr>
<td>policy-map policy-map-name</td>
<td>Creates a policy map by entering the policy map name, and enter the policy-map configuration mode.</td>
</tr>
<tr>
<td>class-{class-map-name class-default}</td>
<td>Enter a child class map name or enter the class-default command to match all the unclassified packets, and enter the policy-map class configuration mode.</td>
</tr>
<tr>
<td>random-detect exponential-weighting-constant exponent</td>
<td>Configures the weight factor used in calculating the average queue length.</td>
</tr>
</tbody>
</table>
When you enable WRED with the `random-detect` interface configuration command, the parameters are set to their default values. The weight factor is 9. For all precedences, the mark probability denominator is 10, and the maximum threshold is based on the output buffering capacity and the transmission speed for the interface.

The default minimum threshold depends on the precedence. The minimum threshold for IP precedence 0 corresponds to half the maximum threshold for the interface. Repeat this command for each precedence. To configure RED rather than WRED, use the same parameters for each precedence.

- For `bytes` bytes, enter the maximum threshold in bytes. The default depends on the interface speed. The minimum and maximum range is 1 to 4096.

Hierarchical Policy Maps Configuration Examples

These are examples of using policy maps to configure hierarchical QoS.

Configure policy maps `phb` and `vlan`:

```
Switch(config)# policy-map phb
Switch(config-pmap)# class cos1
Switch(config-pmap-c)# shape average 1000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cos2
Switch(config-pmap-c)# shape average 2000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit

Switch(config)# policy-map vlan
Switch(config-pmap)# class vlan1
Switch(config-pmap-c)# shape average 5000
```

When you enable WRED with the `random-detect` interface configuration command, the parameters are set to their default values. The weight factor is 9. For all precedences, the mark probability denominator is 10, and the maximum threshold is based on the output buffering capacity and the transmission speed for the interface.

The default minimum threshold depends on the precedence. The minimum threshold for IP precedence 0 corresponds to half the maximum threshold. The values for the remaining precedences fall between half the maximum threshold and the maximum threshold at evenly spaced intervals.
Chapter 27  Configuring Quality of Service (QoS)

Configuring QoS

Switch(config-pmap-c)# service-policy phb
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# class vlan2
Switch(config-pmap-c)# shape average 6000
Switch(config-pmap-c)# service-policy phb
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# exit

This is an example of a policy on a port to address Port-Shaper when EFP policies are present:

Switch(config)# policy-map port-policy
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# policy-map efp-policy
Switch(config-pmap-c)# class class-default
Switch(config-pmap-c)# shape average percent 25
Switch(config-pmap-c)# service-policy child-policy
Switch(config-pmap-c)# exit

This is an example of a 3-level output policy. You can attach this policy only to physical ports and not to EFP service instances.

Switch(config)# policy-map interface-policy-with-vlan-child
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 10000
Switch(config-pmap-c)# service-policy vlan-policy
Switch(config-pmap-c)# exit

This is an example of a 2-level output policy. You can attach this policy to physical ports or to EFP service instances.

Switch(config)# policy-map interface-policy-with-phb-child
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 10000
Switch(config-pmap-c)# service-policy phb
Switch(config-pmap-c)# exit

This is an example of a 2-level output policy. You can attach this policy to physical ports or to EFP service instances.

Switch(config)# policy-map interface-policy-with-phb-child
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# service-policy vlan-policy
Switch(config-pmap-c)# exit

Configuring MPLS and EoMPLS QoS

- Default MPLS and EoMPLS QoS Configuration, page 27-69
- MPLS QoS Configuration Guidelines, page 27-69
- Setting the Priority of Packets with Experimental Bits, page 27-69
- MPLS DiffServ Tunneling Modes, page 27-71
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 VLAN and port-based EoMPLS packets is to use a value of 0 in the EXP bits of the virtual-connection and tunnel labels. The default behavior for L3VPN MPLS packets is to relay the IP Precedence bits into 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.

MPLS QoS Configuration Guidelines

- The switch supports these MPLS QoS features:
  - MPLS can tunnel the QoS values of a packet (that is, QoS is transparent from edge to edge). With QoS transparency, the IP marking in the IP packet is preserved across the MPLS network.
  - You can mark the MPLS EXP field differently and separately from the per-hop behavior (PHB) marked in the IP precedence, DSCP, or CoS field.
- One label-switched path (LSP) can support up to eight classes of traffic (that is, eight PHBs) because the MPLS EXP field is a 3-bit field.
- MPLS DiffServ tunneling modes support E-LSPs. An E-LSP is an LSP on which nodes determine the QoS treatment for MPLS packet exclusively from the EXP bits in the MPLS header.
- The switch does not support egress QoS marking.
- MPLS QoS classification does not work for bridged MPLS packets.
- For port-based EoMPLS, you cannot match the payload VLAN.

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.

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.
- Configure a policy map to mark MPLS packets (write their classification into the MPLS experimental field).
- Attach the service policy to the input interface or service instance.

Beginning in privileged EXEC mode, follow these steps to set the experimental bits for EoMPLS or MPLS QoS:

<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>class-map class-map-name</td>
<td>Specify the name of the traffic class, and enter class-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.

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 in-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 input in-policy
Switch(config-if)# end
```
MPLS DiffServ Tunneling Modes

The switch supports MPLS DiffServ tunneling modes, which allows QoS to be transparent from one edge of a network to the other edge. A tunnel starts where there is label imposition and ends where there is label disposition.

The switch supports three tunneling modes:

- uniform mode
- short-pipe mode
- pipe mode

For additional information, see “MPLS DiffServ Tunneling Modes” at this URL:


Attaching a Service Policy to an Interface or EFP

You use the `service-policy` interface configuration command to attach a service policy to an interface or EFP (service instance) and to specify the direction in which the policy should be applied: either an input policy map for incoming traffic or an output policy map for outgoing traffic. Input and output policy maps support different QoS features.

You can attach a service policy to a physical port or to an EFP. However, you cannot attach a service policy to a physical port that has EFPs configured. If you try to configure an EFP on a switchport that has a service policy attached, the service policy is detached. However, when EFPs are configured on a physical port, you can attach a port policy with a class-default shaper configuration.

Note

If you enter the `no policy-map` configuration command or the `no policy-map policy-map-name` global configuration command to delete a policy map that is attached to an interface or EFP, a warning message that lists the interfaces from which the policy map is being detached is displayed. For example:

Warning: Detaching Policy test1 from Interface GigabitEthernet0/1
The policy map is then detached and deleted.

Beginning in privileged EXEC mode, follow these steps to attach a policy map to a 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><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>service-policy { input</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show policy-map [policy-map-name] [class class-map-name]</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To remove the policy map and port association, use the `no service-policy { input | output } policy-map-name` interface configuration command.
Beginning in privileged EXEC mode, follow these steps to attach a policy map to an EFP:

<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 attach to the policy map, and enter interface configuration mode. Valid interfaces are physical ports.</td>
</tr>
<tr>
<td>Step 3</td>
<td>service instance number ethernet [name] Configure an EFP (service instance) and enter service-instance configuration mode. See Chapter 12, “Configuring Ethernet Virtual Connections (EVCs).”</td>
</tr>
<tr>
<td></td>
<td>Note You must enter the switchport mode trunk and switchport trunk allowed vlan none interface configuration commands on an interface before configuring an EFP. You must also enter the no ip igmp-snooping vlan vlan-id command for the VLAN of the bridge domain.</td>
</tr>
<tr>
<td>Step 4</td>
<td>encapsulation {default</td>
</tr>
<tr>
<td></td>
<td>Note You must configure encapsulation type and a bridge domain for the service instance, or the service-policy command will be rejected.</td>
</tr>
<tr>
<td>Step 5</td>
<td>bridge-domain bridge-id [split-horizon group group-id] Configure the bridge domain ID. The range is from 1 to 8000.</td>
</tr>
<tr>
<td>Step 6</td>
<td>service-policy {input</td>
</tr>
<tr>
<td>Step 7</td>
<td>end Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 8</td>
<td>show ethernet service instance policy-map Verify your entries.</td>
</tr>
<tr>
<td>Step 9</td>
<td>copy running-config startup-config (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove the policy map and port association, use the no service-policy {input | output} policy-map-name service-instance configuration command.

### Displaying QoS Information

To display QoS information, use one or more of the privileged EXEC commands in Table 27-2. For explanations about available keywords, see the command reference for this release.

<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-map information for all class maps or the specified class map.</td>
</tr>
<tr>
<td>show policy-map [policy-map-name</td>
<td>interface [interface-id] [input</td>
</tr>
</tbody>
</table>
You can use the `show policy-map interface [interface-id]` privileged EXEC command to show input and output policy map statistics per classification. Statistics include the number of packets that match each specified traffic stream, the corresponding configured action, such as policing or scheduling, and the associated statistics.

This is an example of the output of the `show policy-map interface` command showing statistics for an output policy map.

```
Switch# show policy-map interface gigabitethernet 0/2
GigabitEthernet0/2

Service-policy output: phb

Class-map: phb (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: cos 2
  Bandwidth 1000 (kbps)
  Queue-limit current-queue-depth 0 bytes
  Output Queue:
    Tail Packets Drop: 0
    Tail Bytes Drop: 0

Class-map: class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any
```
Configuring EtherChannels

This chapter describes how to configure EtherChannels on Layer 2 and Layer 3 ports on the Cisco ME 3800X and ME 3600X 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.

Note: Although EtherChannels are not supported on ports configured with service instances, you can configure a service instance on an EtherChannel port channel.

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

- Understanding EtherChannels, page 28-1
- Configuring EtherChannels, page 28-8
- Displaying EtherChannel, PAgP, and LACP Status, page 28-20

Understanding EtherChannels

- EtherChannel Overview, page 28-1
- Port-Channel Interfaces, page 28-3
- Port Aggregation Protocol, page 28-4
- Link Aggregation Control Protocol, page 28-5
- EtherChannel On Mode, page 28-6
- Load Balancing and Forwarding Methods, page 28-6

EtherChannel Overview

An EtherChannel consists of individual ports bundled into a single logical link as shown in Figure 28-1.
Understanding EtherChannels

Figure 28-1 Typical EtherChannel Configuration

The EtherChannel provides full-duplex bandwidth of up to 800 Mbps between your switch and another switch or host for Fast EtherChannel on a switch with 24 Fast Ethernet ports. For Gigabit EtherChannel, you can configure up to 8 Gbps (8 ports of 1 Gbps), depending on the number of supported Gigabit Ethernet interfaces.

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. The number of EtherChannels is limited to 48. For more information, see the “EtherChannel Configuration Guidelines” section on page 28-9. 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 10, “Configuring Interfaces.”

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.

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 changes to the remaining links within the EtherChannel. A trap is sent for a failure, identifying 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 28-2.

Each EtherChannel has a port-channel logical interface numbered from 1 to 48. This port-channel interface number corresponds to the one specified with the `channel-group` interface configuration command.

**Figure 28-2  Relationship of Physical Ports, Logical Port Channels, and Channel Groups**
Understanding EtherChannels

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. Configuration changes applied to the physical port affect only the port to which you apply the configuration. To change the parameters of all ports in an EtherChannel, apply the configuration commands to the port-channel interface.

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 28-1 shows the user-configurable EtherChannel PAgP modes for the channel-group interface configuration command on an port.

<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 that is 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**

Cisco Discovery Protocol (CDP) sends and receives 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 standard and enables Cisco switches to manage Ethernet channels between switches that conform to the standard. 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 28-2 shows the user-configurable EtherChannel LACP modes for the `channel-group` interface configuration command on a port.

<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 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 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 CDP sends and receives 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. It can be useful if the remote device does not support PAgP or LACP. With the **on** mode, a usable EtherChannel exists only when 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 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.

The switch supports load distribution based on the destination host MAC address supports for only four ports per EtherChannel. When you configure EtherChannel destination-MAC address load balancing, the traffic is balanced only among four ports in the channel group. If you configure more than four ports in an EtherChannel with destination host MAC address load distribution, only four of the ports receive distributed traffic. This limitation does not apply to the other load distribution methods.

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 28-3, 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.
Configuring EtherChannels

- Default EtherChannel Configuration, page 28-9
- EtherChannel Configuration Guidelines, page 28-9
- Configuring Layer 2 EtherChannels, page 28-10 (required)
- Configuring Layer 3 EtherChannels, page 28-12 (required)
- Configuring EtherChannel Load Balancing, page 28-15 (optional)
- Configuring the PAgP Learn Method and Priority, page 28-16 (optional)
- Configuring LACP Hot-Standby Ports, page 28-17 (optional)
- EtherChannels and Ethernet Flow Points (EFPs), page 28-19 (optional)

**Note**
Make sure that the ports are correctly configured. For more information, see the “EtherChannel Configuration Guidelines” section on page 28-9.

**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 to which you apply the configuration.
Default EtherChannel Configuration

Table 28-3 shows the 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.</td>
</tr>
<tr>
<td>PAgP priority</td>
<td>128.</td>
</tr>
<tr>
<td>LACP mode</td>
<td>No default.</td>
</tr>
<tr>
<td>LACP learn method</td>
<td>Aggregate-port learning.</td>
</tr>
<tr>
<td>LACP port priority</td>
<td>32768.</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:

- Do not try to configure more than 26 EtherChannels on the switch.
- 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. ME 3800X and ME 3600X ports are enabled by default.
- 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 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.
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.
- You cannot assign a port configured with a service instance to an EtherChannel.
- If you configure an EtherChannel from trunk ports, verify that the trunking mode 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.

- For configuring Ethernet Virtual Connections (EVCs), you can add a service instance to an EtherChannel port 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.

Note: Although you cannot assign a port configured with an EFP service instance to an EtherChannel, you can configure service instances on EtherChannel port channels.

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>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 a physical port, and enter interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>For a PAgP EtherChannel, you can configure up to eight ports of the same type and speed for the same group.</td>
</tr>
<tr>
<td></td>
<td>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></td>
<td>Note: An EtherChannel port cannot be a port configured with a service instance.</td>
</tr>
<tr>
<td>Step 3</td>
<td></td>
</tr>
<tr>
<td>switchport mode {access</td>
<td>trunk}</td>
</tr>
<tr>
<td>switchport access vlan vlan-id</td>
<td>If you configure the port as a static-access port, assign it to only one VLAN. The range is 1 to 4094.</td>
</tr>
</tbody>
</table>
To remove a port from the EtherChannel group, use the `no channel-group` interface configuration command.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>channel-group channel-group-number mode</code> { auto [ non-silent ]</td>
<td>Assign the port to a channel group, and specify the PAgP or the LACP mode.</td>
</tr>
<tr>
<td>desirable [ non-silent ]</td>
<td>(For channel-group-number, the range is 1 to 26.)</td>
</tr>
<tr>
<td>on</td>
<td>For <code>channel-group-number</code>, the range is 1 to 26.</td>
</tr>
<tr>
<td>{ active</td>
<td>passive }</td>
</tr>
<tr>
<td>--auto</td>
<td>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.</td>
</tr>
<tr>
<td>--desirable</td>
<td>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.</td>
</tr>
<tr>
<td>--on</td>
<td>Forces the port to channel without PAgP or LACP. With the <code>on</code> mode, a usable EtherChannel exists only when a port group in the <code>on</code> mode is connected to another port group in the <code>on</code> mode.</td>
</tr>
<tr>
<td>--non-silent</td>
<td>(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 <code>auto</code> or <code>desirable</code> mode. If you do not specify <code>non-silent</code>, 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.</td>
</tr>
<tr>
<td>--active</td>
<td>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.</td>
</tr>
<tr>
<td>--passive</td>
<td>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.</td>
</tr>
<tr>
<td>For information on compatible modes for the switch and its partner, see the “PAgP Modes” section on page 28-4 and the “LACP Modes” section on page 28-5.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>end</th>
<th>Return to privileged EXEC mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td>show running-config</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>
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:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable non-silent
Switch(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:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(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>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 | `interface port-channel` port-channel-number | Specify the port-channel logical interface, and enter interface configuration mode.  
For `port-channel-number`, the range is 1 to 26. |
| Step 3 | `ip address` ip-address mask                | Assign an IP address and subnet mask to the EtherChannel.              |
| Step 4 | `end`                                        | Return to privileged EXEC mode.                                         |
| Step 5 | `show etherchannel` channel-group-number detail | Verify your entries.                                                   |
| Step 6 | `copy running-config startup-config`        | (Optional) Save your entries in the configuration file.                |
| Step 7 |                                              | Assign an Ethernet port to the Layer 3 EtherChannel. For more information, see the “Configuring the Physical Interfaces” section on page 28-13. |
To remove the port-channel, use the **no interface port-channel port-channel-number** global configuration command.

This example shows how to create the 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></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>no ip address</strong></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>no switchport</strong></td>
</tr>
</tbody>
</table>
### Configuring EtherChannels

**Step 5**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`channel-group channel-group-number mode {auto [non-silent]</td>
<td>desirable [non-silent]</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

For information on compatible modes for the switch and its partner, see the “PAgP Modes” section on page 28-4 and the “LACP Modes” section on page 28-5.

**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 your entries.</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>
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 gigabitethernet0/1-2
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 28-6.

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><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>port-channel load-balance {dst-ip</td>
</tr>
<tr>
<td></td>
<td>dst-ip—Load distribution is based on the destination-host IP address.</td>
</tr>
<tr>
<td></td>
<td>dst-mac—Load distribution is based on the destination-host MAC address of the incoming packet.</td>
</tr>
<tr>
<td></td>
<td>src-dst-ip—Load distribution is based on the source-and-destination host-IP address.</td>
</tr>
<tr>
<td></td>
<td>src-dst-mac—Load distribution is based on the source-and-destination host-MAC address.</td>
</tr>
<tr>
<td></td>
<td>src-ip—Load distribution is based on the source-host IP address.</td>
</tr>
<tr>
<td></td>
<td>src-mac—Load distribution is based on the source-MAC address of the incoming packet.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show etherchannel load-balance</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

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.

**Note**
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.

When the link partner to the switch is a physical learner, we recommend that you configure the Cisco ME 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 physical learner 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><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>Specify the port for transmission, and enter interface configuration mode.</td>
</tr>
</tbody>
</table>
Configuring EtherChannels

To return the priority to its default setting, use the `no pagp port-priority` interface configuration command. By default, **aggregation-port learning** 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 **physical-port** to connect with another switch that is a physical learner. Make sure to configure the `port-channel load-balance` global configuration command to **src-mac** as described in the “Configuring EtherChannel Load Balancing” section on page 28-15.

The learning method must be configured the same at both ends of the link.

### 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td><code>pagp learn-method physical-port</code></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 <code>port-channel load-balance</code> global configuration command to <strong>src-mac</strong> as described in the “Configuring EtherChannel Load Balancing” section on page 28-15. The learning method must be configured the same at both ends of the link.</td>
</tr>
<tr>
<td>4</td>
<td><code>pagp port-priority priority</code></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>
<tr>
<td>5</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>6</td>
<td><code>show running-config</code></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td></td>
<td>or <code>show pagp channel-group-number internal</code></td>
<td></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>

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.
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 28-18 and the “Configuring the LACP Port Priority” section on page 28-18.

### 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>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>lacp system-priority <code>priority</code></td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show running-config</td>
</tr>
<tr>
<td>or</td>
<td>show lacp sys-id</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</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>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Specify the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>lACP port-priority priority</td>
<td>Configure the LACP port priority.</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>show lacp [channel-group-number]internal</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 return the LACP port priority to the default value, use the **no lACP port-priority** interface configuration command.

**EtherChannels and Ethernet Flow Points (EFPs)**

For an LACP or PAgP port to peer with a neighbor on a port that has an Ethernet Virtual Connection (EVC) EFP service instance configured, you need to enter the **l2 protocol peer lACP** or **l2 protocol peer lACP** service-instance configuration command on the service instance. See the “Configuring Ethernet Virtual Connections (EVCs)” chapter for more information on EFPs.

This example shows how to configure Layer 2 protocol LACP peer on a service instance:

```
Switch (config)# interface gigabitethernet0/1
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan none
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# encapsulation untagged
Switch (config-if-srv)# l2protocol peer lACP
Switch (config-if-srv)# bridge-domain 10
Switch (config-if-srv)# end
```
Displaying EtherChannel, PAgP, and LACP Status

To display EtherChannel, PAgP, and LACP status information, use the privileged EXEC commands described in Table 28-4:

Table 28-4 Commands for Displaying EtherChannel, PAgP, and LACP Status

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show etherchannel</td>
<td>Displays EtherChannel information in a brief, detailed, and one-line summary form. Also displays the load-balance or frame-distribution scheme, port, port-channel, and protocol information.</td>
</tr>
<tr>
<td>show pagp</td>
<td>Displays PAgP information such as traffic information, the internal PAgP configuration, and neighbor information.</td>
</tr>
<tr>
<td>show lacp</td>
<td>Displays LACP information such as traffic information, the internal LACP configuration, and neighbor information.</td>
</tr>
</tbody>
</table>

You can clear PAgP channel-group information and traffic counters by using the `clear pagp {channel-group-number} counters` privileged EXEC command.

You can clear LACP channel-group information and traffic counters by using the `clear lacp {channel-group-number} counters` privileged EXEC command.

For detailed information about the fields in the displays, see the command reference for this release.
Configuring IP Unicast Routing

This chapter describes how to configure IP Version 4 (IPv4) unicast routing on the Cisco ME 3800X and ME 3600X switch. For more detailed IPv4 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 has these sections:

- Understanding IP Routing, page 29-1
- Steps for Configuring Routing, page 29-2
- Configuring IP Addressing, page 29-3
- Enabling IPv4 Unicast Routing, page 29-16
- Configuring RIP, page 29-17
- Configuring OSPF, page 29-22
- Configuring EIGRP, page 29-33
- Configuring BGP, page 29-41
- Configuring ISO CLNS Routing, page 29-61
- Configuring BFD, page 29-71
- Configuring Multi-VRF CE, page 29-82
- Configuring Protocol-Independent Features, page 29-95
- Monitoring and Maintaining the IP Network, page 29-106

Understanding IP Routing

In an IP network, each subnetwork is mapped to an individual VLAN. 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 29-1 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.
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, finds 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.

### Types of Routing

Routers and Layer 3 switches can route packets in three different ways:

- **By using default routing**—sending traffic with a destination unknown to the router to a default outlet or destination.
- **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**

### Steps for Configuring Routing

By default, IPv4 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 28-12.
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 29-4.

Configuring IPv4g 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 IPv4 routing on the switch.
- Assign IPv4 addresses to the Layer 3 interfaces.
- Enable selected routing protocols on the switch.
- Configure routing protocol parameters (optional).

**Configuring IP Addressing**

IP routing requires that Layer 3 network interfaces are assigned IP addresses to enable the interfaces and to allow communication with the hosts on 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 29-3
- Assigning IP Addresses to Network Interfaces, page 29-4
- Configuring Address Resolution Methods, page 29-7
- Routing Assistance When IP Routing is Disabled, page 29-10
- Configuring Broadcast Packet Handling, page 29-12
- Monitoring and Maintaining IP Addressing, page 29-16

### 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>
</tbody>
</table>
Configuring IP Addressing

Assigning IP Addresses to Network Interfaces

An IP address identifies a location to which IP packets can be sent. 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 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
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:

1. configure terminal
2. ip subnet-zero
3. end
4. show running-config
5. copy running-config startup-config

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 29-2, 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 29-2  IP Classless Routing

In Figure 29-3, 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 29-3  No IP Classless Routing

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>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 no ip classless</td>
<td>Disable classless routing behavior.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Chapter 29      Configuring IP Unicast Routing

Configuring IP Addressing

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. To communicate with a device on Ethernet, the software must learn the MAC address of the device. The process of learning the MAC address from an IP address is called address resolution. The process of learning 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 learns 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 learn 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.

The switch also uses 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 29-7
- **Set ARP Encapsulation**, page 29-9
- **Enable Proxy ARP**, page 29-9

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

---

**Command** | **Purpose**
--- | ---
show running-config | Verify your entry.

**Step 4**

**Step 5**

`copy running-config startup-config` | *(Optional) Save your entry in the configuration file.*
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>arp ip-address hardware-address type</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>arp ip-address hardware-address type [alias]</td>
</tr>
<tr>
<td>Step 4</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 5</td>
<td>arp timeout seconds</td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
</tr>
<tr>
<td>Step 7</td>
<td>show interfaces [interface-id]</td>
</tr>
<tr>
<td>Step 8</td>
<td>show arp</td>
</tr>
<tr>
<td></td>
<td>or show ip arp</td>
</tr>
<tr>
<td>Step 9</td>
<td>copy running-config startup-config</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><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>interface interface-id</code> Enter interface configuration mode, and specify the Layer 3 interface to configure.</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 learn 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><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>interface interface-id</code> Enter interface configuration mode, and specify the Layer 3 interface to configure.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ip proxy-arp</code> Enable proxy ARP on the interface.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>show ip interface [interface-id]</code> Verify the configuration on the interface or all interfaces.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>copy running-config startup-config</code> (Optional) Save your entries in the configuration file.</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 29-10
- Default Gateway, page 29-10
- ICMP Router Discovery Protocol (IRDP), page 29-10

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 learn 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 29-9. 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>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 default-gateway ip-address</td>
</tr>
<tr>
<td></td>
<td>Set up a default gateway (router).</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 ip redirects</td>
</tr>
<tr>
<td></td>
<td>Display the address of the default gateway router to verify the setting.</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 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
list to Routing Information Protocol (RIP) routing 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 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 ip irdp</td>
<td>Enable IRDP processing on the interface.</td>
</tr>
<tr>
<td>Step 4 ip irdp multicast</td>
<td>(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 ip irdp holdtime seconds</td>
<td>(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 ip irdp maxadvertinterval seconds</td>
<td>(Optional) Set the IRDP maximum interval between advertisements. The default is 600 seconds.</td>
</tr>
<tr>
<td>Step 7 ip irdp minadvertinterval seconds</td>
<td>(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 ip irdp preference number</td>
<td>(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 ip irdp address address [number]</td>
<td>(Optional) Specify an IRDP address and preference to proxy-advertise.</td>
</tr>
<tr>
<td>Step 10 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 11 show ip irdp</td>
<td>Verify settings by displaying IRDP values.</td>
</tr>
<tr>
<td>Step 12 copy running-config startup-config</td>
<td>(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.

**Note**
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 20, “Configuring 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. The switch supports several addressing schemes for forwarding broadcast messages.

- Enabling Directed Broadcast-to-Physical Broadcast Translation, page 29-12
- Forwarding UDP Broadcast Packets and Protocols, page 29-13
- Establishing an IP Broadcast Address, page 29-14
- Flooding IP Broadcasts, page 29-14

Enabling Directed Broadcast-to-Physical Broadcast Translation

By default, IP-directed broadcasts are not forwarded; they are dropped to make 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. 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 26, “Configuring Network Security with ACLs.”

Beginning in privileged EXEC mode, follow these steps to enable forwarding of IP-directed broadcasts on 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 specify the interface to configure.</td>
</tr>
<tr>
<td>3</td>
<td>ip directed-broadcast [access-list-number]</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 an access list is specified, only IP packets permitted by the access list are eligible to be translated.</td>
</tr>
<tr>
<td>4</td>
<td>exit</td>
<td>Return to global configuration mode.</td>
</tr>
</tbody>
</table>
Chapter 29  Configuring IP Unicast Routing

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 that 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 find 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 configure 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.

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>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 helper-address address</td>
</tr>
</tbody>
</table>
## Configuring IP Unicast Routing

### Configuring IP Addressing

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> 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 interface to configure.</td>
</tr>
<tr>
<td><strong>Step 3</strong> ip broadcast-address ip-address</td>
<td>Enter a broadcast address different from the default, for example 128.1.255.255.</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 ip interface [interface-id]</td>
<td>Verify the broadcast address on the interface or all interfaces.</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 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, the interface can receive broadcasts but it never forwards the 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 so it 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><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>ip forward-protocol spanning-tree</code></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 running-config</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>copy running-config startup-config</code></td>
</tr>
</tbody>
</table>

Use the `no ip forward-protocol spanning-tree` global configuration command to disable the flooding of IP broadcasts.

In the 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:

<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 forward-protocol turbo-flood</code></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 running-config</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>copy running-config startup-config</code></td>
</tr>
</tbody>
</table>

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 29-2 Commands to Clear Caches, Tables, and Databases

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear arp-cache</td>
<td>Clear the IP ARP cache and the fast-switching cache.</td>
</tr>
<tr>
<td>clear host {name</td>
<td>Remove one or all entries from the hostname and the address cache.</td>
</tr>
<tr>
<td>clear ip route {network [mask</td>
<td>Remove one or more routes from the IP routing table.</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 29-3 Commands to Display Caches, Tables, and Databases

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show arp</td>
<td>Display the entries in the ARP table.</td>
</tr>
<tr>
<td>show hosts</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>show ip aliases</td>
<td>Display IP addresses mapped to TCP ports (aliases).</td>
</tr>
<tr>
<td>show ip arp</td>
<td>Display the IP ARP cache.</td>
</tr>
<tr>
<td>show ip interface [interface-id]</td>
<td>Display the IP status of interfaces.</td>
</tr>
<tr>
<td>show ip irdp</td>
<td>Display IRDP values.</td>
</tr>
<tr>
<td>show ip masks address</td>
<td>Display the masks used for network addresses and the number of subnets using each mask.</td>
</tr>
<tr>
<td>show ip redirects</td>
<td>Display the address of a default gateway.</td>
</tr>
<tr>
<td>show ip route [address [mask] l [protocol]</td>
<td>Display the current state of the routing table.</td>
</tr>
<tr>
<td>show ip route summary</td>
<td>Display the current state of the routing table in summary form.</td>
</tr>
</tbody>
</table>

### Enabling IPv4 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>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.</td>
</tr>
</tbody>
</table>
Chapter 29       Configuring IP Unicast Routing

Configuring RIP

The Routing Information Protocol (RIP) is an interior gateway protocol (IGP) used in small, homogeneous networks. It is a distance-vector routing protocol that uses broadcast User Datagram Protocol (UDP) data packets to exchange routing information. 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.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>router ip_routing_protocol</strong></td>
<td>Specify an IP routing protocol. This step might include other commands, such as specifying the networks to route with the <strong>network (RIP)</strong> 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</td>
<td><strong>end</strong></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td><strong>show running-config</strong></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6</td>
<td><strong>copy running-config startup-config</strong></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 CNTL/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 29-17
- Configuring OSPF, page 29-22
- Configuring EIGRP, page 29-33
- Configuring BGP, page 29-41
- Configuring ISO CLNS Routing, page 29-61
- Configuring BFD for OSPF, page 29-76
- Configuring Protocol-Independent Features, page 29-95 (optional)
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, but is treated by RIP as a network to implement default routing. 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.

These sections contain this configuration information:

- Default RIP Configuration, page 29-18
- Configuring Basic RIP Parameters, page 29-18
- Configuring RIP Authentication, page 29-20
- Configuring Split Horizon, page 29-20

## 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 <code>version</code> router configuration command.</td>
</tr>
<tr>
<td>IP RIP send version</td>
<td>According to the <code>version</code> router configuration command.</td>
</tr>
<tr>
<td>IP RIP triggered</td>
<td>According to the <code>version</code> 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>
<tr>
<td>Offset list</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Output delay</td>
<td>0 milliseconds.</td>
</tr>
<tr>
<td>Timers basic</td>
<td>• Update: 30 seconds.</td>
</tr>
<tr>
<td></td>
<td>• Invalid: 180 seconds.</td>
</tr>
<tr>
<td></td>
<td>• Hold-down: 180 seconds.</td>
</tr>
<tr>
<td></td>
<td>• Flush: 240 seconds.</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 Basic RIP Parameters

To configure RIP, you enable RIP routing for a network and optionally configure other parameters. On the Cisco ME 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>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 rip</td>
<td>Enable a RIP routing process, and enter router configuration mode.</td>
</tr>
<tr>
<td>4</td>
<td>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. <strong>Note</strong> You must configure a network number for RIP commands to take effect.</td>
</tr>
<tr>
<td>5</td>
<td>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>6</td>
<td>offset list [access-list number</td>
<td>(Optional) Apply an offset list to routing metrics to increase incoming and outgoing metrics to routes learned through RIP. You can limit the offset list with an access list or an interface.</td>
</tr>
<tr>
<td></td>
<td>name] {in</td>
<td>out} offset [type number]</td>
</tr>
</tbody>
</table>
| 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. |
| 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. |
| 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. |
| 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. |
| 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. |
Configuring RIP

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 specifies 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 29-105.

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: 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 configure.</td>
</tr>
<tr>
<td>Step 3: ip rip authentication key-chain name-of-chain</td>
<td>Enable RIP authentication.</td>
</tr>
<tr>
<td>Step 4: ip rip authentication mode [text</td>
<td>md5]</td>
</tr>
<tr>
<td>Step 5: end</td>
<td>Return to privileged EXEC mode.</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 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 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 when links are broken.
In general, Cisco does 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 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 configure.</td>
</tr>
<tr>
<td>Step 3 ip address ip-address subnet-mask</td>
<td>Configure the IP address and IP subnet.</td>
</tr>
<tr>
<td>Step 4 no ip split-horizon</td>
<td>Disable split horizon on the interface.</td>
</tr>
<tr>
<td>Step 5 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6 show ip interface interface-id</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 enable the split horizon mechanism, use the `ip split-horizon` interface configuration command.

### Configuring Summary Addresses

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:

<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 ip address ip-address subnet-mask</td>
<td>Configure the IP address and IP subnet.</td>
</tr>
<tr>
<td>Step 4 ip summary-address rip ip address ip-network mask</td>
<td>Configure the IP address to be summarized and the IP network mask.</td>
</tr>
<tr>
<td>Step 5 no ip split horizon</td>
<td>Disable split horizon on the interface.</td>
</tr>
<tr>
<td>Step 6 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 7 show ip interface interface-id</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>

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 interface Gigabit Ethernet port 2, and 10.0.0.0 is not advertised. If the interface is 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.

```
Switch(config)# router rip
Switch(config-router)# interface gi0/2
Switch(config-if)# no switchport
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 OSPF**

Open Shortest Path First (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.

This section briefly describes how to configure 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. The switch supports all these network types.

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.
These sections contain this configuration information:

- Default OSPF Configuration, page 29-23
- Nonstop Forwarding Awareness, page 29-24
- Configuring OSPF Interfaces, page 29-25
- Configuring OSPF Network Types, page 29-27
- Configuring OSPF Area Parameters, page 29-29
- Configuring Other OSPF Parameters, page 29-30
- Changing LSA Group Pacing, page 29-31
- Configuring a Loopback Interface, page 29-32
- Monitoring OSPF, page 29-33

Default OSPF Configuration

Table 29-5  Default OSPF Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
</table>
| Interface parameters     | Cost: No default cost predefined.  
Retransmit interval: 5 seconds.  
Transmit delay: 1 second.  
Priority: 1.  
Hello interval: 10 seconds.  
Dead interval: 4 times the hello interval.  
No authentication.  
No password specified.  
MD5 authentication disabled. |
| Area                     | Authentication type: 0 (no authentication).  
Default cost: 1.  
Range: Disabled.  
Stub: No stub area defined.  
NSSA: No NSSA area defined. |
| Auto cost                | 100 Mbps.                                                                      |
| Default-information originate | Disabled. When enabled, the default metric setting is 10, and the external route type default is Type 2. |
| Default metric           | Built-in, automatic metric translation, as appropriate for each routing protocol. |
| Distance OSPF            | dist1 (all routes within an area): 110.  
dist2 (all routes from one area to another): 110.  
and dist3 (routes from other routing domains): 110. |
| OSPF database filter     | Disabled. All outgoing link-state advertisements (LSAs) are flooded to the interface. |
| IP OSPF name lookup      | Disabled.                                                                      |
The OSPF NSF Awareness feature is supported for IPv4 in the metro IP access image. 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. For more information on this feature see the OSPF Nonstop Forwarding (NSF) Awareness document at this URL:


### 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>
<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>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>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>
</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>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Enter interface configuration mode, and specify the Layer 3 interface to configure.</td>
</tr>
<tr>
<td>ip ospf cost</td>
<td>(Optional) Explicitly specify the cost of sending a packet on the interface.</td>
</tr>
<tr>
<td>ip ospf retransmit-interval seconds</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>
</tbody>
</table>
### Configuring OSPF

<table>
<thead>
<tr>
<th>Step 5</th>
<th><code>ip ospf transmit-delay seconds</code></th>
<th>(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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td><code>ip ospf priority number</code></td>
<td>(Optional) Set priority to help find the OSPF designated router for a network. The range is from 0 to 255. The default is 1.</td>
</tr>
<tr>
<td>Step 7</td>
<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>Step 8</td>
<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>
<tr>
<td>Step 9</td>
<td><code>ip ospf authentication-key key</code></td>
<td>(Optional) Assign a password to be used by neighboring OSPF routers. The password can be any string of keyboard-entered characters up to 8 bytes in length. All neighboring routers on the same network must have the same password to exchange OSPF information.</td>
</tr>
</tbody>
</table>
| Step 10| `ip ospf message digest-key keyid md5 key` | (Optional) Enable MDS authentication.  
  - `keyid`—An identifier from 1 to 255.  
  - `key`—An alphanumeric password of up to 16 bytes. |
| Step 11| `ip ospf database-filter all out` | (Optional) Block flooding of OSPF LSA packets to the interface. By default, OSPF floods new LSAs over all interfaces in the same area, except the interface on which the LSA arrives. |
| Step 12| `end`                           | Return to privileged EXEC mode. |
| Step 13| `show ip ospf interface [interface-name]` | Display OSPF-related interface information. |
| Step 14| `show ip ospf neighbor detail`   | Display NSF awareness status of neighbor switch. The output matches one of these examples:  
  - `Options is 0x52`  
    - `LLS Options is 0x1 (LR)`  
      When both of these lines appear, the neighbor switch is NSF aware.  
  - `Options is 0x42`—This means the neighbor switch is not NSF aware. |
| Step 15| `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 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>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>neighbor ip-address [priority number] [poll-interval seconds]</td>
</tr>
<tr>
<td></td>
<td>ip-address——Enter the interface IP address of the OSPF neighbor.</td>
</tr>
<tr>
<td></td>
<td>(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.</td>
</tr>
<tr>
<td></td>
<td>(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).</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show ip ospf [process-id]</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

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.
Chapter 29      Configuring IP Unicast Routing

Configuring OSPF

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>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>
</tbody>
</table>
| **Step 3** ip ospf network {broadcast | Configures the OSPF network type for the specified interface. Select one of these network types:
| non-broadcast | broadcast—Specify an OSPF broadcast multi-access network. |
| point-to-multipoint | non-broadcast—Specify an OSPF NBMA network. |
| point-to-point | point-to-multipoint—Specify an OSPF point-to-multipoint network. If you do not enter another keyword, the interface is point-to-multipoint for broadcast media. |
| non-broadcast | point-to-multipoint non-broadcast—Specify an OSPF nonbroadcast point-to-multipoint network. |
| point-to-point | point-to-point—Specify an OSPF point-to-point network. |
| **Step 4** exit | Return to global configuration mode. |
| **Step 5** router ospf process-id | (Optional for point-to-multipoint; required for point-to-multipoint nonbroadcast) Configure an OSPF routing process and enter router configuration mode. |
| **Step 6** neighbor ip-address cost number | (Optional for point-to-multipoint; required for point-to-multipoint nonbroadcast). Specify a configured OSPF neighbor and assign a cost to the neighbor. |
| | - ip-address—Enter the interface IP address of the OSPF neighbor. |
| | - cost number—Specify a cost for the neighbor as an integer from 1 to 65535. |
| **Note** | On point-to-multipoint broadcast networks, specifying a neighbor is optional, but if you do specify a neighbor, you must specify a cost for that neighbor. On point-to-multipoint nonbroadcast neighbors, you must specify a neighbor, but assigning a cost to the neighbor is optional. If not specified, neighbors assume the cost of the interface, based on the ip ospf cost interface configuration command. |
| **Step 7** end | Return to privileged EXEC mode. |
| **Step 8** show ip ospf interface [interface-id] | Display OSPF-related interface information. |
| **Step 9** copy running-config startup-config | (Optional) Save your entries in the configuration file. |

Use the no form of the ip ospf network command to return to the default network type for the media.
Chapter 29  Configuring IP Unicast Routing

Configuring OSPF

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 no-summary 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 29-99, 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 specified 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>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>router ospf process-id</code></td>
<td>Enable OSPF routing, and enter router configuration mode.</td>
</tr>
</tbody>
</table>
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></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>router ospf process-id</td>
</tr>
<tr>
<td></td>
<td>Enable OSPF routing, and enter router configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>timers lsa-group-pacing seconds</td>
</tr>
<tr>
<td></td>
<td>Change the group pacing of LSAs.</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 configuration file.</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>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 loopback 0</td>
</tr>
<tr>
<td></td>
<td>Create a loopback interface, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip address address mask</td>
</tr>
<tr>
<td></td>
<td>Assign an IP address to this interface.</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 ip interface</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 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 29-6 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>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></td>
</tr>
<tr>
<td>show ip ospf border-routes</td>
<td>Display the internal OSPF routing ABR and ASBR table entries.</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

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.
EIGRP 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 by periodically sending small hello packets. As long as hello packets are received, the neighbor is alive and functioning. When this status is determined, the neighboring routers 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, 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. To ensure low convergence time, the reliable transport sends multicast packets quickly when there are unacknowledged packets pending.

- **The DUAL finite state machine** handles the decision process for all route computations. It tracks all routes advertised by all neighbors and 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 to determine a new successor. The amount of time it takes to recompute the route affects the convergence time. When a topology change occurs, DUAL tests for feasible successors 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. Routing decisions are stored in the IP routing table. EIGRP also redistributes routes learned by other IP routing protocols.

These sections contain this configuration information:

- Default EIGRP Configuration, page 29-35
- Configuring Basic EIGRP Parameters, page 29-36
- Configuring EIGRP Interfaces, page 29-37
- Configuring EIGRP Route Authentication, page 29-38
- Configuring EIGRP Stub Routing, page 29-39
- Monitoring and Maintaining EIGRP, page 29-40
# Default EIGRP Configuration

## Table 29-7, Part 1  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>NSF(^1) Awareness</td>
<td>Enabled(^2). 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 switches running the metro IP access image.
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.

Nonstop Forwarding Awareness

The EIGRP NSF Awareness feature is supported for IPv4 in the metro IP access image. 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><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>router eigrp autonomous-system</td>
</tr>
<tr>
<td></td>
<td>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><strong>Step 3</strong></td>
<td>network network-number</td>
</tr>
<tr>
<td></td>
<td>Associate networks with an EIGRP routing process. EIGRP sends updates to the interfaces in the specified networks.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>eigrp log-neighbor-changes</td>
</tr>
<tr>
<td></td>
<td>(Optional) Enable logging of EIGRP neighbor changes to monitor routing system stability.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>metric weights tos k1 k2 k3 k4 k5</td>
</tr>
<tr>
<td></td>
<td>(Optional) Adjust the EIGRP metric. Although the defaults have been carefully set to provide excellent operation in most networks, you can adjust them.</td>
</tr>
<tr>
<td></td>
<td>Caution Setting metrics is complex and is not recommended without guidance from an experienced network designer.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>offset list [access-list number</td>
</tr>
<tr>
<td></td>
<td>(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>
<tr>
<td><strong>Step 7</strong></td>
<td>no auto-summary</td>
</tr>
<tr>
<td></td>
<td>(Optional) Disable automatic summarization of subnet routes into network-level routes.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>ip summary-address eigrp autonomous-system-number address mask</td>
</tr>
<tr>
<td></td>
<td>(Optional) Configure a summary aggregate.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Use the no forms of these commands to disable the feature or return the setting to the default value.

### 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><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 bandwidth-percent eigrp percent</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ip summary-address eigrp autonomous-system-number address mask</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>ip hello-interval eigrp autonomous-system-number seconds</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>ip hold-time eigrp autonomous-system-number seconds</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>no ip split-horizon eigrp autonomous-system-number</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>show ip eigrp interface</td>
</tr>
<tr>
<td><strong>Step 10</strong></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.

**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></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>ip authentication mode eigrp autonomous-system md5</strong></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>ip authentication key-chain eigrp autonomous-system key-chain</strong></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>key chain name-of-chain</strong></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>key number</strong></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>key-string text</strong></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>**accept-lifetime start-time {infinite</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>**send-lifetime start-time {infinite</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td><strong>show key chain</strong></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td><strong>copy running-config startup-config</strong></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. 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.

### 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.

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 29-4, 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 29-4  EIGRP Stub Router Configuration**

Chapter 29      Configuring IP Unicast Routing

Beginning in privileged EXEC mode, follow these steps to configure a remote or spoke router for EIGRP stub 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 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 network network-number</td>
<td>Associate networks with an EIGRP routing process.</td>
</tr>
<tr>
<td>Step 4 eigrp stub [receive-only</td>
<td>connected</td>
</tr>
<tr>
<td></td>
<td>• Enter receive-only to set the router as a receive-only neighbor.</td>
</tr>
<tr>
<td></td>
<td>• Enter connected to advertise connected routes.</td>
</tr>
<tr>
<td></td>
<td>• Enter static to advertise static routes.</td>
</tr>
<tr>
<td></td>
<td>• Enter summary to advertise summary routes.</td>
</tr>
<tr>
<td>Step 5 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6 show ip eigrp neighbor detail</td>
<td>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.</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>

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 29-8** 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>
<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>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 for loop-free exchanges 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.

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.

For details about BGP commands and keywords, see the “IP Routing Protocols” part of 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 15.1(2)EY.”

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 29-5 shows a network that is running both EBGP and IBGP.

Figure 29-5 EBGP, IBGP, and Multiple Autonomous Systems

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 29-5, 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 29-49 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.

- Default BGP Configuration, page 29-43
- Enabling BGP Routing, page 29-45
- Managing Routing Policy Changes, page 29-47
- Configuring BGP Decision Attributes, page 29-49
- Configuring BGP Filtering with Route Maps, page 29-51
- Configuring BGP Filtering by Neighbor, page 29-52
- Configuring Prefix Lists for BGP Filtering, page 29-53
- Configuring BGP Community Filtering, page 29-54
- Configuring BGP Neighbors and Peer Groups, page 29-56
- Configuring Aggregate Addresses, page 29-58
- Configuring Routing Domain Confederations, page 29-58
- Configuring Route Dampening, page 29-59
- Monitoring and Maintaining BGP, page 29-60

For detailed descriptions of BGP configuration, see the “Configuring BGP” chapter in the “IP Routing Protocols” part of 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 Release 15.1(2)EY.”
## 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>
<tr>
<td>Best path</td>
<td>• The router considers <em>as-path</em> in choosing a route and does not compare similar routes from external BGP peers.</td>
</tr>
<tr>
<td></td>
<td>• Compare router ID: Disabled.</td>
</tr>
<tr>
<td>BGP community list</td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Format: Cisco default format (32-bit number).</td>
</tr>
<tr>
<td>BGP confederation identifier/peers</td>
<td>• Identifier: None configured.</td>
</tr>
<tr>
<td></td>
<td>• Peers: None identified.</td>
</tr>
<tr>
<td>BGP Fast external fallover</td>
<td>Enabled.</td>
</tr>
<tr>
<td>BGP local preference</td>
<td>100. The range is 0 to 4294967295 with the higher value preferred.</td>
</tr>
<tr>
<td>BGP network</td>
<td>None specified; no backdoor route advertised.</td>
</tr>
<tr>
<td>BGP route dampening</td>
<td>Disabled by default. When enabled:</td>
</tr>
<tr>
<td></td>
<td>• Half-life is 15 minutes.</td>
</tr>
<tr>
<td></td>
<td>• Re-use is 750 (10-second increments).</td>
</tr>
<tr>
<td></td>
<td>• Suppress is 2000 (10-second increments).</td>
</tr>
<tr>
<td></td>
<td>• Max-suppress-time is 4 times half-life; 60 minutes.</td>
</tr>
<tr>
<td>BGP router ID</td>
<td>The IP address of a loopback interface if one is configured or the highest IP address configured for a physical interface on the router.</td>
</tr>
<tr>
<td>Default information originate (protocol or network redistribution)</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Default metric</td>
<td>Built-in, automatic metric translations.</td>
</tr>
<tr>
<td>Distance</td>
<td>• External route administrative distance: 20 (acceptable values are from 1 to 255).</td>
</tr>
<tr>
<td></td>
<td>• Internal route administrative distance: 200 (acceptable values are from 1 to 255).</td>
</tr>
<tr>
<td></td>
<td>• Local route administrative distance: 200 (acceptable values are from 1 to 255).</td>
</tr>
<tr>
<td>Distribute list</td>
<td>• In (filter networks received in updates): Disabled.</td>
</tr>
<tr>
<td></td>
<td>• Out (suppress networks from being advertised in updates): Disabled.</td>
</tr>
<tr>
<td>Internal route redistribution</td>
<td>Disabled.</td>
</tr>
<tr>
<td>IP prefix list</td>
<td>None defined.</td>
</tr>
</tbody>
</table>
Table 29-9  Default BGP Configuration (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
</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                             | • 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. |
| Neighbor                             | • 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\(^1\) Awareness                  | Disabled\(^2\). 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.                                                                        |
| Table map update                     | Disabled.                                                                       |
| Timers                               | Keepalive: 60 seconds; holdtime: 180 seconds.                                    |

1. NSF = Nonstop Forwarding
2. BGP NSF Awareness can be enabled for IPv4 on switches with the metro IP access image by enabling Graceful Restart.
Nonstop Forwarding Awareness

The BGP NSF Awareness feature is supported for IPv4 in the metro IP access image. 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 must pass traffic through it from another AS to a third AS, it is important to be consistent about the routes it advertises. If BGP advertises a route before all routers in the network learn about the route through the IGP, the AS might receive traffic that some routers can 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:

<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 routing</td>
<td>Enable IP routing (required only if IP routing is disabled).</td>
</tr>
<tr>
<td>Step 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>Step 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>
</tbody>
</table>
Configuring BGP

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 29-5.

**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 specify where to send updates.

For detailed descriptions of BGP configuration, see the “IP Routing Protocols” part of 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 Release 15.1(2)EY,” 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. The switch supports a soft reset without any prior configuration when both BGP peers 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 29-10  Advantages and Disadvantages of Hard and Soft Resets**

<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</td>
<td>Both BGP routers must support the route refresh capability.</td>
</tr>
<tr>
<td></td>
<td>Does not require storing of routing table updates and has no memory overhead</td>
<td></td>
</tr>
</tbody>
</table>

Beginning in privileged EXEC mode, follow these steps to learn if a BGP peer supports the route refresh capability and to reset the BGP session:

**Command Purpose**

**Step 1**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| show ip bgp neighbors | Display whether a neighbor supports the route refresh capability. When supported, this message appears for the router:  
Received route refresh capability from peer. |

**Step 2**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| clear ip bgp { * | address | peer-group-name} | Reset the routing table on the specified connection.  
• Enter an asterisk (*) to specify that all connections be reset.  
• Enter an IP address to specify the connection to be reset.  
• Enter a peer group name to reset the peer group. |

**Step 3**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| clear ip bgp { * | address | peer-group-name} soft out | (Optional) Perform an outbound soft reset to reset the inbound routing table on the specified connection. Use this command if route refresh is supported.  
• Enter an asterisk (*) to specify that all connections be reset.  
• Enter an IP address to specify the connection to be reset.  
• Enter a peer group name to reset the peer group. |

**Step 4**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip bgp</td>
<td>Verify the reset by checking information about the routing table and about BGP neighbors.</td>
</tr>
<tr>
<td>show ip bgp neighbors</td>
<td></td>
</tr>
</tbody>
</table>

**BFD Support for Static Routing**

Unlike dynamic routing protocols, such as OSPF and BGP, static routing has no method of peer discovery. Therefore, when BFD is configured, the reachability of the gateway is completely dependent on the state of the BFD session to the specified neighbor. Unless the BFD session is up, the gateway for the static route is considered unreachable, and therefore, the affected routes will not be installed in the appropriate Routing Information Base (RIB).
For a BFD session to be successfully established, BFD must be configured on the interface on the peer and a BFD client must be registered on the peer for the address of the BFD neighbor. When an interface is used by dynamic routing protocols, the latter requirement is usually met by configuring the routing protocol instances on each neighbor for BFD. When an interface is used exclusively for static routing, this requirement must be met by configuring static routes on the peers.

If a BFD configuration is removed from the remote peer while the BFD session is in the Up state, the updated state of the BFD session is not signaled to IPv4 static. This causes the static route to remain in the RIB. The only workaround is to remove the IPv4 static BFD neighbor configuration so that the static route no longer tracks the BFD session state. Also, if you change the encapsulation type on a serial interface to one that is unsupported by BFD, BFD will be in a Down state on that interface. The workaround is to shut down the interface, change to a supported encapsulation type, and then reconfigure BFD.

A single BFD session can be used by an IPv4 static client to track the reachability of next hops through a specific interface. You can assign a BFD group for a set of BFD-tracked static routes. Each group must have one active static BFD configuration, one or more passive BFD configurations, and the corresponding static routes to be tracked for BFD. Nongroup entries are BFD-tracked static routes for which a BFD group is not assigned. A BFD group must accommodate static BFD configurations that can be part of different VRFs. Effectively, the passive static BFD configurations need not be in the same VRF as that of the active configuration.

For each BFD group, there can be only one active static BFD session. You can configure the active BFD session by adding a static BFD configuration and a corresponding static route that uses the BFD configuration. The BFD session in a group is created only when there is an active static BFD configuration and a static route that uses the static BFD configuration. When the active static BFD configuration or the active static route is removed from a BFD group, all the passive static routes are withdrawn from the RIB. Effectively, all the passive static routes are inactive until an active static BFD configuration and a static route to be tracked by the active BFD session are configured in the group.

Similarly, for each BFD group, there can be one or more passive static BFD configurations and the corresponding static routes to be tracked for BFD. Passive static session routes take effect only when the active BFD session state is reachable. Though the active BFD session state of the group is reachable, the passive static route is added to the RIB only if the corresponding interface state is Up. When a passive BFD session is removed from a group, it will not affect the active BFD session, if one exists, or the BFD group reachability status.

### Configuring BGP Decision Attributes

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. The decision is based on the value of attributes that the update contains and other BGP-configurable factors. The selected path is entered into the BGP routing table and propagated to its neighbors.

When a BGP peer learns two EGBP 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 EGBP paths are learned from the same neighboring autonomous systems, 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. 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.

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 these 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><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>router bgp autonomous-system</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>bgp best-path as-path ignore</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>`neighbor {ip-address</td>
</tr>
</tbody>
</table>
### Configuring BGP Filtering with Route Maps

Within BGP, you can use route maps 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 29-99 for more information about route maps. Each route map has a name that identifies the route map (map tag) and an optional sequence number.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>`neighbor {ip-address</td>
<td>peer-group-name} weight<code>&lt;br&gt;</code>weight`</td>
</tr>
<tr>
<td>6</td>
<td><code>default-metric number</code></td>
<td>(Optional) Set a MED metric to set preferred paths to external neighbors. All routes without a MED will also be set to this value. The range is 1 to 4294967295. The lowest value is the most desirable.</td>
</tr>
<tr>
<td>7</td>
<td><code>bgp bestpath med missing-as-worst</code></td>
<td>(Optional) Configure the switch to consider a missing MED as having a value of infinity, making the path without a MED value the least desirable.</td>
</tr>
<tr>
<td>8</td>
<td><code>bgp always-compare med</code></td>
<td>(Optional) Configure the switch to compare MEDs for paths from neighbors in different autonomous systems. By default, MED comparison is only done among paths in the same AS.</td>
</tr>
<tr>
<td>9</td>
<td><code>bgp bestpath med confed</code></td>
<td>(Optional) Configure the switch to consider the MED in choosing a path from among those advertised by different subautonomous systems within a confederation.</td>
</tr>
<tr>
<td>10</td>
<td><code>bgp deterministic med</code></td>
<td>(Optional) Configure the switch to consider the MED variable when choosing among routes advertised by different peers in the same AS.</td>
</tr>
<tr>
<td>11</td>
<td><code>bgp default local-preference value</code></td>
<td>(Optional) Change the default local preference value. The range is 0 to 4294967295; the default value is 100. The highest local preference value is preferred.</td>
</tr>
<tr>
<td>12</td>
<td><code>maximum-paths number</code></td>
<td>(Optional) Configure the number of paths to be added to the IP routing table. The default is to only enter the best path in the routing table. The range is from 1 to 8. Having multiple paths allows load balancing among the paths.</td>
</tr>
<tr>
<td>13</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>14</td>
<td><code>show ip bgp</code> &lt;br&gt;<code>show ip bgp neighbors</code></td>
<td>Verify the reset by checking information about the routing table and about BGP neighbors.</td>
</tr>
<tr>
<td>15</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the **no** form of each command to return to the default state.
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>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>route-map map-tag [[permit</td>
</tr>
<tr>
<td>Step 3</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>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show route-map [map-name]</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

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 29-103 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 access-list 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>
</tbody>
</table>
Chapter 29  Configuring IP Unicast Routing

Configuring BGP

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. (See the “Regular Expressions” appendix in the Cisco IOS Dial Technologies Command Reference, Release 12.2 for more information on forming regular expressions.) 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>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>neighbor {ip-address</td>
<td>peer-group name} distribute-list {access-list-number</td>
</tr>
<tr>
<td>4</td>
<td>neighbor {ip-address</td>
<td>peer-group name} route-map map-tag {in</td>
</tr>
<tr>
<td>5</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>6</td>
<td>show ip bgp neighbors</td>
<td>Verify the configuration.</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>

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.

<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 as-path access-list access-list-number {permit</td>
<td>deny} as-regular-expressions</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} filter-list {access-list-number</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show ip bgp neighbors [paths regular-expression]</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 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. 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></td>
<td>- network/len is the network number and length (in bits) of the network mask.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) ge and le values specify the range of the prefix length to be matched. The specified ge-value and le-value must satisfy this condition: len &lt; ge-value &lt; le-value &lt; 32</td>
</tr>
<tr>
<td>Step 3: ip prefix-list list-name seq seq-value deny</td>
<td>(Optional) Add an entry to a prefix list, and assign a sequence number to the entry.</td>
</tr>
<tr>
<td></td>
<td>permit network/len [ge ge-value] [le le-value]</td>
</tr>
<tr>
<td>Step 4: end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5: show ip prefix list [detail</td>
<td>Verify the configuration by displaying information about a prefix list or prefix list entries.</td>
</tr>
<tr>
<td></td>
<td>summary] name [network/len] [seq seq-num] [longer] [first-match]</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 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-listseq seq-value** global configuration command. To disable automatic generation of sequence numbers, use the **no ip prefix-listsequence number** command; to reenable automatic generation, use the **ip prefix-listsequence number** command. To clear the hit-count table of prefix list entries, use the **clear ip prefix-list** privileged EXEC command.

### Configuring BGP Community Filtering

One way that BGP controls the distribution of routing information based on the value of the COMMUNITIES attribute. 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 29-99.

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><strong>Step 1</strong></td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ip community-list community-list-number {permit</td>
</tr>
<tr>
<td></td>
<td>• The community-list-number is an integer from 1 to 99 that 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 route-map configuration command.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>router bgp autonomous-system Enter BGP router configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>neighbor {ip-address</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>set comm-list list-num delete</td>
</tr>
<tr>
<td></td>
<td>(Optional) Display and parse BGP communities in the format AA:NN. A BGP community is displayed in a two-part format 2 bytes long. The Cisco default community format is in the format NNAA. In the most recent RFC for BGP, a community takes the form AA:NN, where the first part is the AS number and the second part is a 2-byte number.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>exit Return to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>ip bgp-community new-format</td>
</tr>
<tr>
<td></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 Cisco default community format is in the format NNAA. In the most recent RFC for BGP, a community takes the form AA:NN, where the first part is the AS number and the second part is a 2-byte number.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>end Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Configuring BGP Neighbors and Peer Groups

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.

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><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>router bgp autonomous-system</code> Enter BGP router configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>neighbor peer-group-name peer-group</code> Create a BGP peer group.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>neighbor ip-address peer-group peer-group-name</code> Make a BGP neighbor a member of the peer group.</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>
</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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 11 neighbor {ip-address</td>
<td>peer-group-name} local-as number</td>
</tr>
<tr>
<td>Step 12 neighbor {ip-address</td>
<td>peer-group-name} advertisement-interval seconds</td>
</tr>
<tr>
<td>Step 13 neighbor {ip-address</td>
<td>peer-group-name} maximum-prefix maximum [threshold]</td>
</tr>
<tr>
<td>Step 14 neighbor {ip-address</td>
<td>peer-group-name} next-hop-self</td>
</tr>
<tr>
<td>Step 15 neighbor {ip-address</td>
<td>peer-group-name} password string</td>
</tr>
<tr>
<td>Step 16 neighbor {ip-address</td>
<td>peer-group-name} route-map map-name {in</td>
</tr>
<tr>
<td>Step 17 neighbor {ip-address</td>
<td>peer-group-name} send-community</td>
</tr>
</tbody>
</table>
| Step 18 neighbor {ip-address | peer-group-name} timers keepalive holdtime | (Optional) Set timers for the neighbor or peer group.  
  - The `keepalive` interval is the time within which keepalive messages are sent to peers. The range is 1 to 4294967295 seconds; the default is 60.  
  - The `holdtime` is the interval after which a peer is declared inactive after not receiving a keepalive message from it. The range is 1 to 4294967295 seconds; the default is 180. |
| Step 19 neighbor {ip-address | peer-group-name} weight weight | (Optional) Specify a weight for all routes from a neighbor. |
| Step 20 neighbor {ip-address | peer-group-name} distribute-list {access-list-number | name} {in | out} | (Optional) Filter BGP routing updates to or from neighbors, as specified in an access list. |
| Step 21 neighbor {ip-address | peer-group-name} filter-list access-list-number {in | out | weight weight} | (Optional) Establish a BGP filter. |
| Step 22 neighbor {ip-address | peer-group-name} version value | (Optional) Specify the BGP version to use when communicating with a neighbor. |
| Step 23 neighbor {ip-address | peer-group-name} soft-reconfiguration inbound | (Optional) Configure the software to start storing received updates. |
| Step 24 end | Return to privileged EXEC mode. |
| Step 25 show ip bgp neighbors | Verify the configuration. |
| Step 26 copy running-config startup-config | (Optional) Save your entries in the configuration file. |
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</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>router bgp autonomous-system</td>
</tr>
<tr>
<td>Step 3</td>
<td>aggregate-address address mask</td>
</tr>
<tr>
<td>Step 4</td>
<td>aggregate-address address mask as-set</td>
</tr>
<tr>
<td>Step 5</td>
<td>aggregate-address address-mask summary-only</td>
</tr>
<tr>
<td>Step 6</td>
<td>aggregate-address address mask suppress-map map-name</td>
</tr>
<tr>
<td>Step 7</td>
<td>aggregate-address address mask advertise-map map-name</td>
</tr>
<tr>
<td>Step 8</td>
<td>aggregate-address address mask attribute-map map-name</td>
</tr>
<tr>
<td>Step 9</td>
<td>end</td>
</tr>
<tr>
<td>Step 10</td>
<td>show ip bgp neighbors [advertised-routes]</td>
</tr>
<tr>
<td>Step 11</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

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>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 router bgp autonomous-system</td>
<td>Enter BGP router configuration mode.</td>
</tr>
<tr>
<td>Step 3 bgp confederation identifier</td>
<td>Configure a BGP confederation identifier.</td>
</tr>
<tr>
<td>Step 4 bgp confederation peers</td>
<td>Specify the autonomous systems that belong to the confederation and that will be treated as special EBGP peers.</td>
</tr>
<tr>
<td>Step 5 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6 show ip bgp neighbor</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>

**Configuring Route Dampening**

Route flap dampening minimizes 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 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 router bgp autonomous-system</td>
<td>Enter BGP router configuration mode.</td>
</tr>
<tr>
<td>Step 3 bgp dampening</td>
<td>Enable BGP route dampening.</td>
</tr>
<tr>
<td>Step 4 bgp dampening half-life reuse suppress max-suppress route-map</td>
<td>(Optional) Change the default values of route dampening factors.</td>
</tr>
<tr>
<td>Step 5 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6 show ip bgp flap-statistics</td>
<td>(Optional) Monitor the flaps of all paths that are flapping. The statistics are deleted when the route is not suppressed and is stable.</td>
</tr>
<tr>
<td>Step 7 show ip bgp dampened-paths</td>
<td>(Optional) Display the dampened routes, including the time remaining before they are suppressed.</td>
</tr>
<tr>
<td>Step 8 clear ip bgp flap-statistics</td>
<td>(Optional) Clear BGP flap statistics to make it less likely that a route will be dampened.</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 get 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 29-8 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 29-11 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>
</tbody>
</table>
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: 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`.

Note

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. 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 29-62
- Nonstop Forwarding Awareness, page 29-63
- Configuring IS-IS Global Parameters, page 29-65
- Configuring IS-IS Interface Parameters, page 29-68

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>
<tr>
<td>IS-IS type</td>
<td>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.</td>
</tr>
<tr>
<td>Default-information originate</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Log IS-IS adjacency state changes.</td>
<td>Disabled.</td>
</tr>
<tr>
<td>LSP generation throttling timers</td>
<td>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.</td>
</tr>
</tbody>
</table>
Chapter 29  Configuring IP Unicast Routing

Configuring ISO CLNS Routing

Nonstop Forwarding Awareness

The integrated IS-IS NSF Awareness feature is supported for IPv4 in the metro IP access image. 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>Step 1</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>clns routing</td>
<td>Enable ISO connectionless routing on the switch.</td>
</tr>
</tbody>
</table>
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 gigabitethernet0/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config-router)# exit
Switch(config-if)# interface gigabitethernet0/2
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config-router)# exit
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>router isis [area tag]</strong> Enable the IS-IS routing for the specified routing process and enter IS-IS routing configuration mode. (Optional) Use the <em>area tag</em> 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 <strong>is-type</strong> global configuration command.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>net network-entity-title</strong> Configure the NETs for the routing process. If you are configuring multiarea IS-IS, specify a NET for each routing process. You can specify a name for a NET and for an address.</td>
</tr>
</tbody>
</table>
| **Step 5**            | **is-type {level-1 | level-1-2 | level-2-only}** (Optional) You can configure the router to act as a Level 1 (station) router, a Level 2 (area) router for multi-area routing, or both (the default):  
  * level-1 — act as a station router only  
  * level-1-2 — act as both a station router and an area router  
  * level 2 — act as an area router only |
| **Step 6**            | **exit** Return to global configuration mode. |
| **Step 7**            | **interface interface-id** Specify an interface to route IS-IS, 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. |
| **Step 8**            | **ip router isis [area tag]** Configure an IS-IS routing process for ISO CLNS on the interface and attach an area designator to the routing process. |
| **Step 9**            | **clns router isis [area tag]** Enable ISO CLNS on the interface. |
| **Step 10**           | **ip address ip-address-mask** Define the IP address for the interface. An IP address is required on all interfaces in an area enabled for IS-IS if any one interface is configured for IS-IS routing. |
| **Step 11**           | **end** Return to privileged EXEC mode. |
| **Step 12**           | **show isis [area tag] database detail** Verify your entries. |
| **Step 13**           | **copy running-config startup-config** (Optional) Save your entries in the configuration file. |
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 gigabitethernet0/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config-router)# exit

Router C

Switch(config)# clns routing
Switch(config)# router isis
Switch(config-router)# net 49.0001.0000.0000.000c.00
Switch(config-router)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config-router)# exit

Configuring IS-IS Global Parameters

- 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:
### Configuring ISO CLNS Routing

<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>clns routing</td>
<td>Enable ISO connectionless routing on the switch.</td>
</tr>
<tr>
<td>3</td>
<td>router isis</td>
<td>Specify the IS-IS routing protocol and enter router configuration mode.</td>
</tr>
<tr>
<td>4</td>
<td>default-information originate [route-map map-name]</td>
<td>(Optional) Force a default route into the IS-IS routing domain. If you enter <code>route-map</code> <code>map-name</code>, the routing process generates the default route if the route map is satisfied.</td>
</tr>
<tr>
<td>5</td>
<td>ignore-lsp-errors</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>6</td>
<td>area-password password</td>
<td>(Optional) Configure the area authentication password, which is inserted in Level 1 (station router level) LSPs.</td>
</tr>
<tr>
<td>7</td>
<td>domain-password password</td>
<td>(Optional) Configure the routing domain authentication password, which is inserted in Level 2 (area router level) LSPs.</td>
</tr>
<tr>
<td>8</td>
<td>summary-address address mask [level-1</td>
<td>level-1-2</td>
</tr>
<tr>
<td>9</td>
<td>set-overload-bit [on-startup [seconds</td>
<td>wait-for-bgp]]</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>• (Optional) on-startup</strong>—sets the overload bit only on startup. If <code>on-startup</code> is not specified, the overload bit is set immediately and remains set until you enter the <code>no set-overload-bit</code> command. If <code>on-startup</code> is specified, you must enter a number of seconds or <code>wait-for-bgp</code>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>• seconds</strong>—When the <code>on-startup</code> 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>• wait-for-bgp</strong>—When the <code>on-startup</code> 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.</td>
</tr>
<tr>
<td>10</td>
<td>lsp-refresh-interval seconds</td>
<td>(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).</td>
</tr>
<tr>
<td>11</td>
<td>max-lsp-lifetime seconds</td>
<td>(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.</td>
</tr>
</tbody>
</table>
### Command

| Step 12 | lsp-gen-interval [level-1 | level-2]  |
|---------|-------------------------------------------|
|         | lsp-max-wait [lsp-initial-wait          |
|         | lsp-second-wait]                        |

**Purpose:** 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.

| Step 13 | spf-interval [level-1 | level-2]  |
|---------|---------------------|
|         | spf-max-wait [spf-initial-wait |
|         | spf-second-wait] |

**Purpose:** Sets IS-IS shortest path first (SPF) throttling timers.
- **spf-max-wait:** the maximum interval between consecutive SPFPs (in seconds). The range is 1 to 120, the default is 10.
- **spf-initial-wait:** the initial SPF 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 SPF calculation (in milliseconds). The range is 1 to 10000; the default is 5500.

<table>
<thead>
<tr>
<th>Step 14</th>
<th>prc-interval prc-max-wait</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[prc-initial-wait prc-second-wait]</td>
</tr>
</tbody>
</table>

**Purpose:** 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] |

**Purpose:** 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 |

**Purpose:** 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 |

**Purpose:** 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 |

**Purpose:** Return to privileged EXEC mode.

| Step 19 | show clns |

**Purpose:** Verify your entries.

| Step 20 | copy running-config startup-config |

**Purpose:** 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 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.

Interface level parameters:

- 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>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 to be configured and enter interface configuration mode. If the interface is not already configured as a Level 3 interface, enter the no switchport command to put it into Layer 3 mode.</td>
</tr>
<tr>
<td>Step 3  isis metric default-metric [level-1</td>
<td>level-2]</td>
</tr>
</tbody>
</table>
### Configuring ISO CLNS Routing

#### Step 4
isis hello-interval `{seconds | minimal} [level-1 | level-2]`

(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.

- **minimal**—causes the system to compute the hello interval based on the hello multiplier so that the resulting `holdtime` is 1 second.
- **seconds**—the range is from 1 to 65535. The default is 10 seconds.

#### Step 5
isis hello-multiplier `multiplier` `{level-1 | 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.

#### Step 6
isis csnp-interval `seconds` `{level-1 | 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.

#### Step 7
isis retransmit-interval `seconds`

(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.

#### Step 8
isis retransmit-throttle-interval `milliseconds`

(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 `isis lsp-interval` command.

#### Step 9
isis priority `value` `{level-1 | level-2}`

(Optional) Configure the priority to use for designated router election. The range is from 0 to 127. The default is 64.

#### Step 10
isis circuit-type `{level-1 | level-1-2 | level-2-only}`

(Optional) Configure the type of adjacency desired for neighbors on the specified interface (specify the interface circuit type).

- **level-1**—a Level 1 adjacency is established if there is at least one area address common to both this node and its neighbors.
- **level-1-2**—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.
- **level 2**—a Level 2 adjacency is established. If the neighbor router is a Level 1 router, no adjacency is established.

#### Step 11
isis password `password` `{level-1 | 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.

#### Step 12
end

Return to privileged EXEC mode.

#### Step 13
show clns interface `interface-id`

Verify your entries.

#### Step 14
copy running-config startup-config

(Optional) Save your entries in the configuration file.

To return to the default settings, use the `no` forms of the commands.
Monitoring and Maintaining 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 29-13 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 29-13  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-exp</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 [interface-id]</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 29-6 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 29-7 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.
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), 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 echo mode is disabled, control packets are used to detect forwarding failures. Control packets are exchanged at the configured slow-timer rate, which could result in longer failure-detection time. You configure this rate by entering the `bfd slow-timer` global configuration command. The range is from 1000 to 3000 ms; the default rate is every 1000 ms.

You can enable or disable echo processing at a switch interface independent of the BFD neighbor configuration. Disabling echo mode only disables the sending of echo packets by the interface. The fast-switching layer that receives an echo packet always reflects it back to the sender.

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

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 29-72
- Default BFD Configuration Guidelines, page 29-73
- Configuring BFD Session Parameters on an Interface, page 29-73
- Enabling BFD Routing Protocol Clients, page 29-74

### 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.
Default BFD Configuration Guidelines

The switch supports multiple BFD sessions at one time. The number of BFD session supported is dependant on the timer value:
- 50 BFD sessions with 50ms interval
- 150 BFD sessions with 150ms interval
- 200 BFD session with 300ms interval
- 250 BFD sessions with 600ms interval

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. It is not supported on Layer 2 interfaces and pseudowires.
BFD is supported on Etherchannel.
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 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.
BFD is not supported over MPLS with TE/FRR.
Multi-hop BFD is not supported.

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>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>platform bfd allow-svi</td>
</tr>
<tr>
<td></td>
<td>Allows BFD to be configured on a VLAN or SVI</td>
</tr>
<tr>
<td>Step 3</td>
<td>interface interface-id</td>
</tr>
<tr>
<td></td>
<td>Specify an interface for a BFD session, and enter interface configuration mode. Only physical interfaces support BFD.</td>
</tr>
<tr>
<td>Step 4</td>
<td>no switchport</td>
</tr>
<tr>
<td></td>
<td>Remove the interface from Layer 2 configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>ip address ip-address subnet-mask</td>
</tr>
<tr>
<td></td>
<td>Configure the IP address and IP subnet mask.</td>
</tr>
<tr>
<td>Step 6</td>
<td>bfd interval milliseconds min_rx milliseconds multiplier value</td>
</tr>
<tr>
<td></td>
<td>Set BFD parameters for echo packets on the interface.</td>
</tr>
<tr>
<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).</td>
</tr>
<tr>
<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.</td>
</tr>
<tr>
<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>Note</td>
<td>There are no baseline BFD parameter defaults.</td>
</tr>
<tr>
<td>Step 7</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 8</td>
<td>show running-config</td>
</tr>
<tr>
<td></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 9</td>
<td>show bfd neighbor detail</td>
</tr>
<tr>
<td></td>
<td>(Optional) Display the final configured or negotiated values when the session is created with a neighbor.</td>
</tr>
<tr>
<td>Step 10</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 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 Port-Channel, page 29-75
- Configuring BFD Support for SVI, page 29-75
- Configuring BFD for OSPF, page 29-76
- Configuring BFD for IS-IS, page 29-77
- Configuring BFD for BGP, page 29-79
- Configuring BFD for EIGRP, page 29-79
- Configuring BFD for HSRP, page 29-80
• Configuring BFD Support for Static Routing, page 29-81

Configuring BFD for Port-Channel

Perform the steps in this procedure to configure BFD for Port-channel.

<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 port-channel number</td>
<td>Specify the port-channel for a BFD session, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 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>• interval—Specify the rate at which BFD echo packets are sent to BFD peers. The range is from 50 to 999 milliseconds (ms).</td>
</tr>
<tr>
<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.</td>
</tr>
<tr>
<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>Note</td>
<td>There are no baseline BFD parameter defaults.</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 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 7 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Configuring BFD Support for SVI

Perform the steps in this procedure to configure BFD over SVI on a VLAN SVI interface by setting the baseline BFD session parameters on an interface. Repeat the steps in this procedure for each interface over which you want to run BFD sessions to BFD neighbors.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3 platform bfd allow-svi</td>
<td>Enables support for BFD configuration on a VLAN SVI interface.</td>
</tr>
<tr>
<td>Step 4 interface name number</td>
<td>Enters interface configuration mode for the specified VLAN SVI interface.</td>
</tr>
<tr>
<td>Step 5 ip address ip-address mask</td>
<td>Configure the IP address and IP subnet mask.</td>
</tr>
<tr>
<td>Step 6 bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier</td>
<td>Enables BFD on the interface and configures BFD session parameters.</td>
</tr>
</tbody>
</table>
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</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>router ospf process-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>bfd all-interfaces</td>
</tr>
<tr>
<td>Step 4</td>
<td>exit</td>
</tr>
<tr>
<td>Step 5</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 6</td>
<td>ip ospf bfd disable</td>
</tr>
<tr>
<td>Step 7</td>
<td>end</td>
</tr>
<tr>
<td>Step 8</td>
<td>show bfd neighbors [detail]</td>
</tr>
<tr>
<td>Step 9</td>
<td>copy running-config startup-config</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.

### Configuring BFD for OSPF

This is an example of configuring BFD for OSPF on all OSPF interfaces:

```
Step 7: show running-config
Verify the configuration.
Step 8: end
Exits interface configuration mode and returns to privileged EXEC mode.
Step 9: show bfd neighbor detail
(Optional) Display the final configured or negotiated values when the session is created with a neighbor.
Step 10: copy running-config startup-config
(Optional) Save your entries in the configuration file.
```
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>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>Specify an OSPF process, and enter router configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>4</td>
<td>interface interface-id</td>
<td>Specify an interface, and enter interface configuration mode.</td>
</tr>
<tr>
<td>5</td>
<td>ip ospf bfd</td>
<td>Enable BFD on the specified OSPF interface. Repeat Steps 3 and 4 for all</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interfaces on which you want to run BFD sessions.</td>
</tr>
<tr>
<td>6</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>7</td>
<td>show bfd neighbors [detail]</td>
<td>Verify the 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>

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 gigabitethernet0/1
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>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 is-is area-tag</td>
<td>Specify an IS-IS process and enter router configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>bfd all-interfaces</td>
<td>Enable BFD globally on all interfaces associated with the IS-IS routing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>process.</td>
</tr>
<tr>
<td>4</td>
<td>exit</td>
<td>(Optional) Return to global configuration mode if you want to disable BFD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>on one or more IS-IS interfaces.</td>
</tr>
</tbody>
</table>
Chapter 29  Configuring IP Unicast Routing

Configuring BFD

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.

If you only want to run IS-IS BFD on a few interfaces, instead of enabling it globally, you can enter the `isis bfd` interface configuration command on those interfaces. See the next procedure.

**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 is-is 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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<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 router isis</td>
<td>(Optional) Enable IPv4 IS-IS routing on the interface.</td>
</tr>
<tr>
<td>Step 7   isis bfd disable</td>
<td>(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.</td>
</tr>
<tr>
<td>Step 8   end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 9   show bfd neighbors [detail]</td>
<td>Verify the configuration.</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 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 gigabitethernet0/1
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]</td>
</tr>
<tr>
<td></td>
<td>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 follow these 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>
<tr>
<td>Step 4</td>
<td>bfd {all-interfaces</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></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 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>configure terminal</td>
<td>Enter the global configuration mode.</td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Specify an interface for a BFD session and enter the interface configuration mode. Only physical interfaces support BFD.</td>
</tr>
<tr>
<td>ip address ip-address subnet-mask</td>
<td>Configure the IP address and IP subnet mask for the interface.</td>
</tr>
<tr>
<td>standby [group-number] ip [ip-address] [secondary]</td>
<td>Activate HSRP.</td>
</tr>
<tr>
<td>standby bfd</td>
<td>(Optional) Enable HSRP support for BFD on the interface.</td>
</tr>
<tr>
<td>bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier</td>
<td>(Optional) Enables BFD on the interface.</td>
</tr>
<tr>
<td>exit</td>
<td>Return to the global configuration mode.</td>
</tr>
<tr>
<td>standby bfd all-interfaces</td>
<td>(Optional) Enable HSRP support for BFD on all interfaces.</td>
</tr>
<tr>
<td>end</td>
<td>Return to the privileged EXEC mode.</td>
</tr>
<tr>
<td>show standby neighbors</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 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.
**Configuring BFD Support for Static Routing**

Perform this procedure to configure BFD support for static routing. Repeat the steps in this procedure on each BFD neighbor.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
</tr>
<tr>
<td></td>
<td>Enables the privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>interface type number</td>
</tr>
<tr>
<td></td>
<td>Configures an interface and enters the interface configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip address ip-address mask</td>
</tr>
<tr>
<td></td>
<td>Configures an IP address for the interface.</td>
</tr>
<tr>
<td>Step 5</td>
<td>bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier</td>
</tr>
<tr>
<td></td>
<td>Enables BFD on the interface.</td>
</tr>
<tr>
<td>Step 6</td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td>Exits the interface configuration mode and returns to the global configuration mode.</td>
</tr>
<tr>
<td>Step 7</td>
<td>ip route static bfd interface-type interface-number ip-address [group group-name [passive]]</td>
</tr>
<tr>
<td></td>
<td>Specifies a static route BFD neighbor. The interface-type, interface-number, and ip-address arguments are required because BFD support exists only for directly connected neighbors.</td>
</tr>
<tr>
<td>Step 8</td>
<td>ip route [vrf vrf-name] prefix mask [ip-address</td>
</tr>
<tr>
<td></td>
<td>Specifies a static route BFD neighbor.</td>
</tr>
<tr>
<td>Step 9</td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td>Exits the global configuration mode and returns to the privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 10</td>
<td>show ip static route</td>
</tr>
<tr>
<td></td>
<td>(Optional) Displays static route database information.</td>
</tr>
<tr>
<td>Step 11</td>
<td>show ip static route bfd</td>
</tr>
<tr>
<td></td>
<td>(Optional) Displays information about the static BFD configuration from the configured BFD groups and nongroup entries.</td>
</tr>
<tr>
<td>Step 12</td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td>Exits the privileged EXEC mode and returns to the user EXEC mode.</td>
</tr>
</tbody>
</table>

**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 so it sends no echo packets but only sends back echo packets received from a neighbor. When echo mode is disabled, control packets are used to detect forwarding failures. You can configure slow timers to reduce the frequency of BFD control packets.

Beginning in privileged EXEC mode, follow these steps to disable echo mode on a BFD device and to set the slow timer rate:

<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>Enter a BFD interface and enter interface configuration mode.</td>
</tr>
</tbody>
</table>
Step 3  
no bfd echo  
Disable BFD echo mode on the interface. It is enabled by default, but can be disabled independently on BFD neighbors.

Step 4  
exit  
Return to global configuration mode.

Step 5  
bfd slow-timer [milliseconds]  
(Optional) Configure a BFD slow-timer value. The range is from 1000 to 30000 milliseconds. The default is 1000 milliseconds.

Step 6  
end  
Return to privileged EXEC mode.

Step 7  
show bfd neighbors detail  
Verify your entries.

Step 8  
copy running-config startup-config  
(Optional) Save your entries in the configuration file.

To disable 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 an ISP 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.

The switch supports multiple VPN routing/forwarding (multi-VRF) instances in customer edge (CE) devices (multi-VRF CE). With Multi-VRF CE, a service provider can support two or more VPNs with overlapping IP addresses.

- Understanding Multi-VRF CE, page 29-82
- Default Multi-VRF CE Configuration, page 29-84
- Multi-VRF CE Configuration Guidelines, page 29-84
- Configuring VRFs, page 29-85
- Configuring VRF-Aware Services, page 29-86
- Configuring a VPN Routing Session, page 29-89
- Configuring BGP PE to CE Routing Sessions, page 29-90
- Multi-VRF CE Configuration Example, page 29-90
- Displaying Multi-VRF CE Status, page 29-94

### Understanding Multi-VRF CE

Multi-VRF CE 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:

- Customer edge (CE) devices provide customers access to the service-provider network over a data link to one or more provider edge routers. The CE device advertises the site local routes to the router and learns the remote VPN routes from it. The Cisco ME 3400 switch can be a CE.

- Provider edge (PE) routers exchange routing information with CE devices by using static routing or a routing protocol such as BGP, RIPv2, OSPF, 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 (IBGP).

- 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 29-8 shows a configuration using Cisco ME 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 Cisco ME switches. Because multi-VRF CE is a Layer 3 feature, each interface in a VRF must be a Layer 3 interface.

Figure 29-8 Switches Acting as Multiple Virtual CEs

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 (PL) in multi-VRF-CE-related data structures and adds the VLAN ID and PL to the VLAN database.

When 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 strips 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. If 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.
- 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 29-14 shows the default VRF configuration.

#### Table 29-14 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>5000</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 29-8, 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.

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.

The switch supports one global network and up to 26 VRFs.

Most routing protocols (BGP, OSPF, RIP, EIGRP, 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 affect the packet switching rate.

If no VRFs are configured, up to 105 policies can be configured.

If even one VRF is configured than 41 policies can be configured.

If more than 41 policies are configured then VRF cannot be configured.

VRF and private VLANs are mutually-exclusive. You cannot enable VRF on a private VLAN. Similarly, you cannot enable private VLAN on a VLAN with VRF configured on the VLAN interface.

VRF and policy-based routing (PBR) are mutually-exclusive on a switch interface. You cannot enable VRF when PBR is enabled on an interface. In contrast, you cannot enable PBR when VRF is enabled on an interface.

## 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, 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>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>ip routing</td>
<td>Enable IP routing.</td>
</tr>
<tr>
<td>Step 3</td>
<td></td>
</tr>
<tr>
<td>ip vrf vrf-name</td>
<td>Name the VRF, and enter VRF configuration mode.</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;vvpn 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;vvpn 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>
<tr>
<td>5</td>
<td>snmp-server host &lt;host&gt; vrf &lt;vvpn instance&gt; informs &lt;community&gt;</td>
<td>Specify the recipient of an SNMP inform operation and specify the VRF table to be used for sending SNMP informs.</td>
</tr>
<tr>
<td>6</td>
<td>snmp-server user &lt;user&gt; &lt;group&gt; remote &lt;host&gt; vrf &lt;vvpn instance&gt; &lt;security model&gt;</td>
<td>Add a user to an SNMP group for a remote host on a VRF for SNMP access.</td>
</tr>
<tr>
<td>7</td>
<td>end</td>
<td>Return to privileged EXEC mode.</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>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>no switchport</td>
<td>Remove the interface from Layer 2 configuration mode if it is a physical interface.</td>
</tr>
<tr>
<td><strong>Step 4</strong>ip vrf forwarding &lt;vrf-name&gt;</td>
<td>Configure VRF on the interface.</td>
</tr>
<tr>
<td><strong>Step 5</strong>ip address ip address</td>
<td>Enter the IP address for the interface.</td>
</tr>
<tr>
<td><strong>Step 6</strong>standby 1 ip ip address</td>
<td>Enable HSRP and configure the virtual IP address.</td>
</tr>
<tr>
<td><strong>Step 7</strong>end</td>
<td>Return to privileged EXEC mode.</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>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong>logging on</td>
<td>Enable or temporarily disable logging of storage router event message.</td>
</tr>
<tr>
<td><strong>Step 3</strong>logging host ip address vrf vrf name</td>
<td>Specify the host address of the syslog server where logging messages are to be sent.</td>
</tr>
<tr>
<td><strong>Step 4</strong>logging buffered logging buffered size debug</td>
<td>Log messages to an internal buffer.</td>
</tr>
<tr>
<td><strong>Step 5</strong>logging trap debug</td>
<td>Limit the logging messages sent to the syslog server.</td>
</tr>
<tr>
<td><strong>Step 6</strong>logging facility facility</td>
<td>Send system logging messages to a logging facility.</td>
</tr>
<tr>
<td><strong>Step 7</strong>end</td>
<td>Return to privileged EXEC mode.</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.

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>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>ip ftp source-interface interface-type interface-number</td>
<td>Specify the source IP address for FTP connections.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</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></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip tftp source-interface interface-type interface-number</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
</tbody>
</table>

Configuring a VPN Routing Session

Routing within the VPN can be configured with any supported routing protocol (RIP, OSPF, EIGRP, 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></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>router ospf process-id vrf vrf-name</td>
</tr>
<tr>
<td>Step 3</td>
<td>log-adjacency-changes</td>
</tr>
</tbody>
</table>
Chapter 29 Configuring IP Unicast Routing

Configuring Multi-VRF CE

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></td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>router bgp autonomous-system-number</code> 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></td>
<td><code>network network-number mask</code> Specify a network and mask to announce using BGP.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>redistribute ospf process-id match internal</code> Set the switch to redistribute OSPF internal routes.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>network network-number area area-id</code> 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></td>
<td><code>address-family ipv4 vrf vrf-name</code> Define BGP parameters for PE to CE routing sessions, and enter VRF address-family mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>neighbor address remote-as as-number</code> Define a BGP session between PE and CE routers.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>neighbor address activate</code> Activate the advertisement of the IPv4 address family.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><code>show ip bgp [ipv4] [neighbors]</code> Verify BGP configuration.</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><code>copy running-config startup-config</code> (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 delete the BGP routing process. Use the command with keywords to delete routing characteristics.

### Multi-VRF CE Configuration Example

Figure 29-9 is a simplified example of the physical connections in a network similar to that in Figure 29-8. 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 Cisco ME 3400 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. The example also includes commands for configuring traffic to Switch A for a Catalyst 6000 or Catalyst 6500 switch acting as a PE router.

**Figure 29-9  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
```
Configuring Multi-VRF CE

Switch(config-if)# ip address 8.8.2.8 255.255.255.0
Switch(config-if)# exit

Switch(config-if)# interface gigabitethernet0/5
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-if)# interface fastethernet0/8
Switch(config-if)# no shutdown
Switch(config-if)# switchport access vlan 208
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config-if)# interface fastethernet0/11
Switch(config-if)# no shutdown
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 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-if)# 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-if)# 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-if)# 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 vl1
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 vl2
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 vl12
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. Configure the connection 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 fastethernet0/2
Switch(config-if)# no shutdown
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. Configure the connection 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 fastethernet0/1
Switch(config-if)# no shutdown
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 only 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 v1
Router(config-vrf)# rd 100:1
Router(config-vrf)# route-target export 100:1
Router(config-vrf)# route-target import 100:1
Router(config-vrf)# exit
Router(config)# ip vrf v2
Chapter 29 Configuring IP Unicast Routing

Configuring Multi-VRF CE

Router(config-vrf)# rd 100:2
Router(config-vrf)# route-target export 100:2
Router(config-vrf)# route-target import 100:2
Router(config-vrf)# exit

Router(config)# ip cef
Router(config)# interface Loopback1
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 3.3.1.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface Loopback2
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 3.3.2.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface gigabitethernet0.10
Router(config-if)# encapsulation dot1q 10
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 38.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface gigabitethernet0.20
Router(config-if)# encapsulation dot1q 20
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 83.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf v2
Router(config-router-af)# neighbor 83.0.0.8 remote-as 800
Router(config-router-af)# neighbor 83.0.0.8 activate
Router(config-router-af)# network 3.3.2.0 mask 255.255.255.0
Router(config-router-af)# exit
Router(config-router)# address-family ipv4 vrf v1
Router(config-router-af)# neighbor 38.0.0.8 remote-as 800
Router(config-router-af)# neighbor 38.0.0.8 activate
Router(config-router-af)# network 3.3.1.0 mask 255.255.255.0
Router(config-router-af)# end

Displaying Multi-VRF CE Status

You can use the privileged EXEC commands in Table 29-15 to display information about multi-VRF CE configuration and status.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip protocols vrf</td>
<td>Display routing protocol information associated with a VRF.</td>
</tr>
<tr>
<td>show ip route vrf</td>
<td>Display IP routing table information associated with a VRF.</td>
</tr>
<tr>
<td>show ip</td>
<td>Display information about the defined VRF instances.</td>
</tr>
</tbody>
</table>

For more information about the information in the displays, refer to 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.*

These sections contain this configuration information:

- Configuring Cisco Express Forwarding, page 29-95
- Configuring the Number of Equal-Cost Routing Paths, page 29-96
- Configuring Static Unicast Routes, page 29-97
- Specifying Default Routes and Networks, page 29-98
- Using Route Maps to Redistribute Routing Information, page 29-99
- Filtering Routing Information, page 29-102
- Managing Authentication Keys, page 29-105

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 use 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 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.

CEF is enabled globally by default. If for some reason it is disabled, you can re-enable it by using the *ip cef* global configuration command.

The default configuration 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* privileged EXEC command can be useful 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.
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 for software-forwarded traffic 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>ip cef</td>
</tr>
<tr>
<td>Step 3</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip route-cache cef</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Step 6</td>
<td>show ip cef</td>
</tr>
<tr>
<td>Step 7</td>
<td>show cef linecard [detail]</td>
</tr>
<tr>
<td>Step 8</td>
<td>show cef interface [interface-id]</td>
</tr>
<tr>
<td>Step 9</td>
<td>show adjacency</td>
</tr>
<tr>
<td>Step 10</td>
<td>copy running-config startup-config</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 see 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>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>ip route prefix mask {address</td>
<td>interface} [distance]</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show ip route</td>
<td>Display the current state of the routing table to 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>

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 29-16. 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 29-16 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>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...
To 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 learn 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><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>ip default-network</strong> network number</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>show ip route</strong></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>copy running-config startup-config</strong> (Optional)</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 set 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. 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>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    | 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. |
| 3    | match as-path path-list-number | Match a BGP AS path access list. |
| 4    | match community-list community-list-number [exact] | Match a BGP community list. |
| 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. |
| 6    | match metric metric-value | Match the specified route metric. The metric-value can be an EIGRP metric with a specified value from 0 to 4294967295. |
| 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). |
| 8    | match tag tag value [ ...tag-value] | Match the specified tag value in a list of one or more route tag values. Each can be an integer from 0 to 4294967295. |
| 9    | match interface type number [ ...type number] | Match the specified next hop route out one of the specified interfaces. |
| 10   | match ip route-source {access-list-number | access-list-name} [ ...access-list-number | ...access-list-name] | Match the address specified by the specified advertised access lists. |
| 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. |
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.

<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>`router [bgp</td>
</tr>
<tr>
<td>Step 3</td>
<td>`redistribute protocol [process-id] {level-1</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>default-metric number</code> Cause the current routing protocol to use the same metric value for all redistributed routes (BGP, RIP and OSPF).</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>default-metric bandwidth delay reliability loading mtu</code> Cause the EIGRP routing protocol to use the same metric value for all non-EIGRP redistributed routes.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>show route-map</code> Display all route maps configured or only the one specified to verify configuration.</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 disable redistribution, use the `no` form of the commands.

The metrics of one routing protocol do not necessarily translate into the metrics of another. 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.

**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>Step 1</td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>router { bgp</td>
</tr>
<tr>
<td>Step 3</td>
<td>passive-interface interface-id Suppress sending routing updates through the specified Layer 3 interface.</td>
</tr>
<tr>
<td>Step 4</td>
<td>passive-interface default (Optional) Set all interfaces as passive by default.</td>
</tr>
<tr>
<td>Step 5</td>
<td>no passive-interface interface type (Optional) Activate only those interfaces that need to have adjacencies sent.</td>
</tr>
<tr>
<td>Step 6</td>
<td>network network-address (Optional) Specify the list of networks for the routing process. The <code>network-address</code> is an IP address.</td>
</tr>
<tr>
<td>Step 7</td>
<td>end Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 8</td>
<td>copy running-config startup-config (Optional) Save your entries in the configuration file.</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:
Configuring Protocol-Independent Features

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 29-16 on page 29-97 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>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 | rip | eigrp }</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>distribute-list { access-list-number | access-list-name } out { interface-name | routing process | autonomous-system-number }</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>distribute-list { access-list-number | access-list-name } in { type-number }</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</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:

<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>key chain name-of-chain</td>
<td>Identify a key chain, and enter key chain configuration mode.</td>
</tr>
<tr>
<td></td>
<td>key number</td>
<td>Identify the key number. The range is 0 to 2147483647.</td>
</tr>
<tr>
<td></td>
<td>key-string text</td>
<td>Identify the key string. The string can contain from 1 to 80 uppercase and lowercase alphanumeric characters, but the first character cannot be a number.</td>
</tr>
<tr>
<td></td>
<td>accept-lifetime start-time { infinite</td>
<td>end-time</td>
</tr>
<tr>
<td></td>
<td>send-lifetime start-time { infinite</td>
<td>end-time</td>
</tr>
<tr>
<td></td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>show key chain</td>
<td>Display authentication key information.</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 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 29-17 to clear routes or display status:

Table 29-17 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>Clear one or more routes from the IP routing table.</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>Display the current state of the routing table.</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>
<tr>
<td>show ip cache</td>
<td>Display the routing table used to switch IP traffic.</td>
</tr>
<tr>
<td>show route-map {map-name}</td>
<td>Display all route maps configured or only the one specified.</td>
</tr>
</tbody>
</table>
This chapter describes how to configure IPv6 unicast routing on the Cisco ME 3600 and ME 3800 Ethernet Access switch.

For information about configuring IPv4 unicast routing, see Configuring IP Unicast Routing, page 29-1

To use this feature, the switch must be running the metro IP access image. To enable IPv6 routing, you must configure the switch to use a dual IPv4 and IPv6 switch database management (SDM) template. See the Dual IPv4 and IPv6 Protocol Stacks, page 30-4.

For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS documentation referenced in the procedures

- Understanding IPv6, page 30-1
- Configuring IPv6, page 30-6
- Displaying IPv6, page 30-16

Understanding IPv6

The primary reason for using IPv6 is to increase Internet global address space to accommodate the rapidly increasing number of users and applications that require unique global IP addresses. IPv4 uses 32-bit addresses to provide approximately 4 billion available addresses. Large blocks of these addresses are allocated to government agencies and large organizations, and the number of available IP addresses is rapidly decreasing. IPv6 incorporates 128-bit source and destination addresses and can provide significantly more globally unique IP addresses than IPv4.

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 how Cisco Systems implements IPv6, go to this URL:

For information about IPv6 and other features in this chapter
- See the Cisco IOS IPv6 Configuration Guide at this URL:
Understanding IPv6

Use the Search field on Cisco.com to locate 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 see links to multiple documents about static routes.

This section describes IPv6 implementation on the switch. It includes the following topics:

- IPv6 Addresses, page 30-2
- Supported IPv6 Unicast Routing Features, page 30-2
- Unsupported IPv6 Unicast Routing Features, page 30-6

IPv6 Addresses

The ME 3600 and ME 3800 switches support only IPv6 unicast addresses. It does not support local-site 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 an example of 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. This is an example:

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 Library on Cisco.com.

In the “Information About Implementing Basic Connectivity for IPv6” 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

Support for the switch includes expanded address capability, header format simplification, improved support for 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 ME 3600 and ME 3800 switches provide IPv6 routing capability over 802.1Q trunk ports for static routes, 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.

- Path MTU Discovery for IPv6 Unicast, page 30-3
- ICMPv6, page 30-3
- Neighbor Discovery, page 30-3
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 neighbor discovery protocol (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 obtains 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 multi-homed 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 Library on Cisco.com.

**IPv6 Stateless Auto-configuration 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 Library on Cisco.com.

**IPv6 Applications**

The switch has IPv6 support for the following applications:

- Ping, traceroute, Telnet, TFTP, and FTP
- Secure Shell (SSH) over an IPv6 transport
- HTTP server access over IPv6 transport
- DNS resolver for AAAA record types 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 Library on Cisco.com.

**Dual IPv4 and IPv6 Protocol Stacks**

You must use the dual IPv4 and IPv6 template to allocate hardware memory usage to both IPv4 and IPv6 protocols.

Figure 30-1 shows a router forwarding both IPv4 and IPv6 traffic through the same interface, based on the IP packet and destination addresses.
Understanding IPv6

Figure 30-1 Dual IPv4 and IPv6 Support on an Interface

Use the dual IPv4 and IPv6 switch database management (SDM) template to enable IPv6 routing dual stack environments (supporting both IPv4 and IPv6). For more information about the dual IPv4 and IPv6 SDM template, see Configuring SDM Templates, page 8-1

- 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.
- IPv6 QoS is not supported.
- If you do not use IPv6, do not use the dual stack template because it results in less hardware memory availability 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 Library 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 Library 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 OSFP for IPv6” chapter in the Cisco IOS IPv6 Configuration Library 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 waits 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 Library on Cisco.com.

Unsupported IPv6 Unicast Routing Features

- IPv6 policy-based routing
- IPv6 virtual private network (VPN) routing and forwarding (VRF) table support
- 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
- HSRP for IPv6
- SNMP and Syslog over IPv6
- MPLS for IPv6
- ACL for IPv6
- BFD for IPv6
- VRF and VRF-lite for IPv6
- IPv6 Multicast
- RIP for IPv6
- EIGRP IPv6

Configuring IPv6

- Default IPv6 Configuration, page 30-7
- Configuring IPv6 Addressing and Enabling IPv6 Routing, page 30-7
- Configuring Default Router Preference, page 30-9
- Configuring IPv4 and IPv6 Protocol Stacks, page 30-10
- Configuring IPv6 ICMP Rate Limiting, page 30-11
- Configuring CEF for IPv6, page 30-12
- Configuring Static Routing for IPv6, page 30-12
- Configuring OSPF for IPv6, page 30-14
Default IPv6 Configuration

Table 30-1 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</td>
<td>Disabled (IPv4 CEF is enabled by default).</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When IPv6 routing is enabled, CEFv6 is automatically enabled.</td>
</tr>
<tr>
<td>IPv6 addresses</td>
<td>None configured.</td>
</tr>
</tbody>
</table>

Configuring IPv6 Addressing and Enabling IPv6 Routing

Follow these rules or limitations when configuring IPv6 on the switch:

- Be sure to select a dual IPv4 and IPv6 SDM template.
- Not all features discussed in this chapter are supported by the switch. See the “Unsupported IPv6 Unicast Routing Features” section on page 30-6.
- In the `ipv6 address` interface configuration command, 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, 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::0:0:0:1:ff00::/104 for each unicast address assigned to the interface (the address for 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 Library* on Cisco.com.
Complete these steps in privileged EXEC mode, 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>
<tr>
<td><strong>Step 8</strong></td>
<td>ipv6 address ipv6-prefix/prefix length eui-64 or ipv6 address ipv6-address link-local or ipv6 enable</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>ip routing</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>ipv6 unicast-routing</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>show ipv6 interface interface-id</td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

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.

### Configuration Examples

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 is included to show 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 gigabitethernet0/2
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 gigabitethernet0/1
GigabitEthernet0/2 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
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
Hosts use stateless autoconfig for addresses.
```

### 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, router advertisements 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.

Complete these steps in privileged EXEC mode, to configure a DRP for a router on 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 Layer 3 interface on which you want to specify the DRP.</td>
</tr>
<tr>
<td>3</td>
<td>ipv6 nd router-preference {high</td>
<td>medium</td>
</tr>
<tr>
<td>4</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Configuring IPv6

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 gigabitethernet0/1
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 Library* 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.

Complete these steps in privileged EXEC mode, 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><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
</tbody>
</table>
| **Step 2** | sdm prefer dual-ipv4-and-ipv6 {default | routing | vlan} | Select an SDM template that supports IPv4 and IPv6.  
  - `default`—Set the switch to the default template to balance system resources.  
  - `routing`—Set the switch to the routing template to support IPv4 and IPv6 routing, including IPv4 policy-based routing.  
  - `vlan`—Maximize VLAN configuration on the switch with no routing supported in hardware. |
| **Step 3** | end | Return to privileged EXEC mode. |
| **Step 4** | reload | Reload the operating system. |
| **Step 5** | configure terminal | Enter global configuration mode. |
| **Step 6** | ip routing | Enable IPv4 routing on the switch. |
| **Step 7** | ipv6 unicast-routing | Enable forwarding of IPv6 data packets on the switch. |
| **Step 8** | interface interface-id | Enter interface configuration mode, and specify the Layer 3 interface to configure. |
| **Step 9** | no switchport | Remove the interface from Layer 2 configuration mode (if it is a physical interface). |
| **Step 10** | ip address ip-address mask [secondary] | Specify a primary or secondary IPv4 address for the interface. |
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 addresses from an interface, use the **no ipv6 enable** interface configuration command. 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 gigabitethernet0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.99.1 244.244.244.0
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
```

### 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.
Complete these steps in privileged EXEC mode, 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 interval [bucketsize]</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 being added to the bucket. The range is from 0 to 2147483647 milliseconds.</td>
</tr>
<tr>
<td></td>
<td>• bucketsize—(Optional) The maximum number of tokens stored in the bucket. The range is from 1 to 200.</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 [interface-id]</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>
</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, allowing more CPU processing power to be dedicated to packet forwarding. IPv4 CEF is enabled by default. IPv6 CEF is disabled by default, but automatically enabled when you configure IPv6 routing.

To route IPv6 unicast packets, first globally configure forwarding of IPv6 unicast packets by using the **ipv6 unicast-routing** global configuration command. You must also 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, use the **ipv6 cef** global configuration command. You can verify the IPv6 state by using the **show ipv6 cef** privileged EXEC command.

For more information about configuring CEF, see the “Implementing IPv6 Addressing and Basic Connectivity” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

### Configuring Static Routing 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.
- Enable IPv6 on at least one Layer 3 interface by configuring an IPv6 address on the interface.
Complete these steps in privileged EXEC mode, 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>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ipv6 route ipv6-prefix/prefix length {ipv6-address</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 ipv6 static [ipv6-address</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>
</tbody>
</table>
Configuring IPv6

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 to an interface. The route has an administrative distance of 130:

```plaintext
Switch(config)# ipv6 route 2001:0DB8::/32 gigabitethernet0/1 130
```

For more information about configuring static IPv6 routing, see the “Implementing Static Routes for IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

**Configuring OSPF for IPv6**

You can customize OSPF for IPv6 for your network. However, the defaults are set to meet the requirements of most customers and features.

Follow these guidelines:

- Be careful when changing the defaults for IPv6 commands. Doing so 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.

Complete these required and optional steps in privileged EXEC mode, to configure IPv6 OSPF:

<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>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>ipv6 router ospf process-id</code></td>
<td>Enable OSPF router configuration mode for the process. The process ID is the number assigned administratively 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>
### Command

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>`area area-id range {ipv6-prefix/prefix length} [advertise</td>
<td>(Optional) Consolidate and summarize routes at an area boundary.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>not-advertise] [cost cost]`</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>area-id</code>—Identifier of the area about which routes are to be</td>
</tr>
<tr>
<td></td>
<td></td>
<td>summarized. It can be specified as either a decimal value or as an IPv6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>prefix.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>ipv6-prefix/prefix length</code>—The destination IPv6 network and a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>decimal value that shows how many of the high-order contiguous bits of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the address comprise the prefix (the network portion of the address).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A slash mark (/) must precede the decimal value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>advertise</code>—(Optional) Set the address range status to advertise and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to generate a Type 3 summary link-state advertisement (LSA).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>not-advertise</code>—(Optional) Set the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and component networks remain hidden from other networks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>cost</code>—(Optional) Metric or cost for this summary route, which is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>used during OSPF SPF calculation to determine the shortest paths to the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>destination. The value can be 0 to 16777215.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>maximum paths number-paths</code></td>
<td>(Optional) Define the maximum number of equal-cost routes to the same</td>
</tr>
<tr>
<td></td>
<td></td>
<td>destination that IPv6 OSPF should enter in the routing table. The range</td>
</tr>
<tr>
<td></td>
<td></td>
<td>is from 1 to 64, and the default is 16 paths.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>exit</code></td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>interface interface-id</code></td>
<td>Enter interface configuration mode, and specify the Layer 3 interface</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to configure.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>ipv6 ospf process-id area area-id [instance instance-id]</code></td>
<td>Enable OSPF for IPv6 on the interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>instance instance-id</code>—(Optional) Instance identifier.</td>
</tr>
<tr>
<td>Step 8</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 9</td>
<td><code>show ipv6 ospf [process-id] [area-id] interface [interface-id]</code></td>
<td>Display information about OSPF interfaces.</td>
</tr>
<tr>
<td></td>
<td>or <code>show ipv6 ospf [process-id] [area-id]</code></td>
<td>Display general information about OSPF routing processes.</td>
</tr>
<tr>
<td>Step 10</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 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 Library* on Cisco.com.
Displaying IPv6

For complete syntax and usage information on these commands, see the Cisco IOS command reference publications.

Table 30-2 Commands for Monitoring IPv6

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 access-list</td>
<td>Display IPv6 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 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 route</td>
<td>Display IPv6 route table entries.</td>
</tr>
<tr>
<td>show ipv6 routers</td>
<td>Display 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 30-3 Commands for Displaying IPv4 and IPv6 Address Types

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip http server history</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>show ip http server connection</td>
<td>Display the current connections to the HTTP server, including the local and remote IP addresses being accessed.</td>
</tr>
<tr>
<td>show ip http client connection</td>
<td>Display the configuration values for HTTP client connections to HTTP servers.</td>
</tr>
<tr>
<td>show ip http client history</td>
<td>Display a list of the last 20 requests made by the HTTP client to the server.</td>
</tr>
</tbody>
</table>

Configuration Example

This is sample 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:0000:0:1::20B:46FF:FE2F:D940, subnet is 3FFE:0000:0::/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
    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 GigabitEthernet0/11
    3FFE:C000:111:1:20B:46FF:FE2F:D945/128
        receive
    3FFE:C000:168:1::/64
        attached to GigabitEthernet0/43
    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

<output truncated>

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
    GigabitEthernet0/4
    GigabitEthernet0/11
    GigabitEthernet0/12
Redistribution:
    None

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:C101:111:1::/33                        - 0000.0000.0033  REACH G10/13

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 route` privileged EXEC command:

Switch# show ipv6 route
IPv6 Routing Table - 21 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S   ::/0 [1/0]
     via 3FFE:C000:0:7::777
C   3FFE:C000:0:1::64 [0/0]
     via ::, Vlan1
L   3FFE:C000:0:1:20B:46FF:FE2F:D940/128 [0/0]
     via ::, Vlan1
C   3FFE:C000:0:7::/64 [0/0]
     via ::, Vlan7
L   3FFE:C000:0:7:20B:46FF:FE2F:D97F/128 [0/0]
     via ::, Vlan7
C   3FFE:C000:111:1::/64 [0/0]
     via ::, GigabitEthernet0/11
L   3FFE:C000:111:1:20B:46FF:FE2F:D945/128 [0/0]
C   3FFE:C000:168:1::/64 [0/0]
     via ::, GigabitEthernet0/4
L   3FFE:C000:168:1:20B:46FF:FE2F:D94B/128 [0/0]
     via ::, GigabitEthernet0/4
C   3FFE:C000:16A:1::/64 [0/0]
     via ::, Loopback10
L   3FFE:C000:16A:1:20B:46FF:FE2F:D900/128 [0/0]
     via ::, Loopback10

<output truncated>

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
  unreachable: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
  parameter: 0 error, 0 header, 0 option
  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
  unreachable: 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
CHAPTER 31

Configuring Virtual Router Redundancy Protocol

The Virtual Router Redundancy Protocol (VRRP) is an election protocol that dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN, allowing several routers on a multi-access link to utilize the same virtual IP address. A VRRP router is configured to run the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP configuration, one router is elected as the virtual router master, with the other routers acting as backups in case the virtual router master fails. This chapter includes the following topics:

- Information About VRRP, page 31-1
- Configuring VRRP, page 31-7
- Configuration Examples for VRRP, page 31-16

Information About VRRP

- VRRP Operation, page 31-1
- Benefits of VRRP, page 31-3
- Multiple Virtual Router Support, page 31-4
- VRRP Router Priority and Preemption, page 31-4
- VRRP Advertisements, page 31-5
- VRRP Object Tracking, page 31-5
- How Object Tracking Affects the Priority of a VRRP Router, page 31-5
- VRRP Authentication, page 31-6
- ISSU—VRRP, page 31-6
- SSO—VRRP, page 31-7

VRRP Operation

There are several ways a LAN client can determine which router should be the first hop to a particular remote destination. The client can use a dynamic process or static configuration. Examples of dynamic router discovery are as follows:

- Proxy ARP—The client uses Address Resolution Protocol (ARP) to get the destination it wants to reach, and a router responds to the ARP request with its own MAC address.
### Information About VRRP

- **Routing protocol**—The client listens to dynamic routing protocol updates (for example, from Routing Information Protocol [RIP]) and forms its own routing table.
- **IRD\P (ICMP Router Discovery Protocol) client**—The client runs an Internet Control Message Protocol (ICMP) router discovery client.

The dynamic discovery protocols incur some configuration and processing overhead on the LAN client. This could be detrimental also, in the event of a router failure, the process of switching to another router can be slow.

An alternative to dynamic discovery protocols is to statically configure a default router on the client. This approach simplifies client configuration and processing, but creates a single point of failure. If the default gateway fails, the LAN client is limited to communicating only on the local IP network segment and is detached from the rest of the network.

VRRP can solve the static configuration problem. VRRP enables a group of routers to form a single *virtual router*. The LAN clients can then be configured with the virtual router as their default gateway. The virtual router, representing a group of routers, is also known as a VRRP group.

VRRP is supported on Ethernet, Fast Ethernet, BVI, and Gigabit Ethernet interfaces, on MPLS VPNs, VRF-aware MPLS VPNs and VLANs.

Figure 31-1 shows a LAN topology in which VRRP is configured. In this example, Routers A, B, and C are **VRRP routers** (routers running VRRP) that comprise a virtual router. The IP address of the virtual router is the same as that configured for the Ethernet interface of Router A (10.0.0.1).

![Figure 31-1 Basic VRRP Topology](image)

Because the virtual router uses the IP address of the physical Ethernet interface of Router A, Router A assumes the role of the **virtual router master** and is also known as the **IP address owner**. As the virtual router master, Router A controls the IP address of the virtual router and is responsible for forwarding packets sent to this IP address. Clients 1 through 3 are configured with the default gateway IP address of 10.0.0.1.

Routers B and C function as **virtual router backups**. If the master virtual router fails, the router configured with the higher priority will become the virtual router master and provide uninterrupted service for the LAN hosts. When Router A recovers, it becomes the virtual router master again. For more detail on the roles that VRRP routers play and what happens if the virtual router master fails, see the “VRRP Router Priority and Preemption” section later in this document.
Figure 31-2 shows a LAN topology in which VRRP is configured so that Routers A and B share the traffic to and from clients 1 through 4 and that Routers A and B act as virtual router backups to each other if either router fails.

**Figure 31-2 Load Sharing and Redundancy VRRP Topology**

In this topology, two virtual routers are configured. (For more information, see the “Multiple Virtual Router Support” section later in this document.) For virtual router 1, Router A is the owner of IP address 10.0.0.1 and virtual router master, and Router B is the virtual router backup to Router A. Clients 1 and 2 are configured with the default gateway IP address of 10.0.0.1.

For virtual router 2, Router B is the owner of IP address 10.0.0.2 and virtual router master, and Router A is the virtual router backup to Router B. Clients 3 and 4 are configured with the default gateway IP address of 10.0.0.2.

**Benefits of VRRP**

**Redundancy**

VRRP enables you to configure multiple routers as the default gateway router, which reduces the possibility of a single point of failure in a network.

**Load Sharing**

You can configure VRRP in such a way that traffic to and from LAN clients can be shared by multiple routers, thereby sharing the traffic load more equitably among available routers.

**Multiple Virtual Routers**

VRRP supports up to 255 virtual routers (VRRP groups) on a router physical interface, subject to the platform supporting multiple MAC addresses. Multiple virtual router support enables you to implement redundancy and load sharing in your LAN topology.

**Multiple IP Addresses**

The virtual router can manage multiple IP addresses, including secondary IP addresses. Therefore, if you have multiple subnets configured on an Ethernet interface, you can configure VRRP on each subnet.
Information About VRRP

Preemption
The redundancy scheme of VRRP enables you to preempt a virtual router backup that has taken over for a failing virtual router master with a higher priority virtual router backup that has become available.

Authentication
VRRP message digest 5 (MD5) algorithm authentication protects against VRRP-spoofing software and uses the industry-standard MD5 algorithm for improved reliability and security.

Advertisement Protocol
VRRP uses a dedicated Internet Assigned Numbers Authority (IANA) standard multicast address (224.0.0.18) for VRRP advertisements. This addressing scheme minimizes the number of routers that must service the multicasts and allows test equipment to accurately identify VRRP packets on a segment. The IANA assigned VRRP the IP protocol number 112.

VRRP Object Tracking
VRRP object tracking provides a way to ensure the best VRRP router is virtual router master for the group by altering VRRP priorities to the status of tracked objects such as interface or IP route states.

Multiple Virtual Router Support
You can configure up to 255 virtual routers on a physical interface. The actual number of virtual routers that a router interface can support depends on the following factors:

- Router processing capability
- Router memory capability
- Router interface support of multiple MAC addresses

In a topology where multiple virtual routers are configured on a router interface, the interface can act as a master for one virtual router and as a backup for one or more virtual routers.

VRRP Router Priority and Preemption
An important aspect of the VRRP redundancy scheme is VRRP router priority. Priority determines the role that each VRRP router plays and what happens if the virtual router master fails.

If a VRRP router owns the IP address of the virtual router and the IP address of the physical interface, this router will function as a virtual router master.

Priority also determines if a VRRP router functions as a virtual router backup and the order of ascendancy to becoming a virtual router master if the virtual router master fails. You can configure the priority of each virtual router backup with a value of 1 through 254 using the `vrrp priority` command.

For example, if Router A, the virtual router master in a LAN topology, fails, an election process takes place to determine if virtual router backups B or C should take over. If Routers B and C are configured with the priorities of 101 and 100, respectively, Router B is elected to become virtual router master because it has the higher priority. If Routers B and C are both configured with the priority of 100, the virtual router backup with the higher IP address is elected to become the virtual router master.
By default, a preemptive scheme is enabled whereby a higher priority virtual router backup that becomes available takes over for the virtual router backup that was elected to become virtual router master. You can disable this preemptive scheme using the `no vrrp preempt` command. If preemption is disabled, the virtual router backup that is elected to become virtual router master remains the master until the original virtual router master recovers and becomes master again.

**VRRP Advertisements**

The virtual router master sends VRRP advertisements to other VRRP routers in the same group. The advertisements communicate the priority and state of the virtual router master. The VRRP advertisements are encapsulated in IP packets and sent to the IPv4 multicast address assigned to the VRRP group. The advertisements are sent every second by default; the interval is configurable.

Although the VRRP protocol as per RFC 3768 does not support millisecond timers, Cisco routers allow you to configure millisecond timers. You need to manually configure the millisecond timer values on both the primary and the backup routers. The master advertisement value displayed in the `show vrrp` command output on the backup routers is always 1 second because the packets on the backup routers do not accept millisecond values.

You must use millisecond timers where absolutely necessary and with careful consideration and testing. Millisecond values work only under favorable circumstances, and you must be aware that the use of the millisecond timer values restricts VRRP operation to Cisco devices only.

**VRRP Object Tracking**

Object tracking is an independent process that manages creating, monitoring, and removing tracked objects such as the state-of-the-line protocol of an interface. Clients such as the Hot Standby Router Protocol (HSRP), Gateway Load Balancing Protocol (GLBP), and now VRRP register their interest with specific tracked objects and act when the state of an object changes.

Each tracked object is identified by a unique number that is specified on the tracking CLI. Client processes such as VRRP use this number to track a specific object.

The tracking process periodically polls the tracked objects and notes any change of value. The changes in the tracked object are communicated to interested client processes, either immediately or after a specified delay. The object values are reported as either up or down.

VRRP object tracking gives VRRP access to all the objects available through the tracking process. The tracking process provides the ability to track individual objects such as the state of an interface line protocol, state of an IP route, or the reachability of a route.

VRRP provides an interface to the tracking process. Each VRRP group can track multiple objects that may affect the priority of the VRRP router. Specify the object number to be tracked and VRRP will be notified of any change to the object. VRRP increments (or decrements) the priority of the virtual router based on the state of the object being tracked.

**How Object Tracking Affects the Priority of a VRRP Router**

The priority of a device can change dynamically if it has been configured for object tracking and the object that is being tracked goes down. The tracking process periodically polls the tracked objects and notes any change of value. The changes in the tracked object are communicated to VRRP, either immediately or after a specified delay. The object values are reported as either up or down. Examples of objects that can be tracked are the line protocol state of an interface or the reachability of an IP route. If
Information About VRRP

the specified object goes down, the VRRP priority is reduced. The VRRP router with the higher priority can now become the virtual router master if it has the `vrrp preempt` command configured. See the “VRRP Object Tracking” section for more information on object tracking.

VRRP Authentication

VRRP ignores unauthenticated VRRP protocol messages. The default authentication type is text authentication.

You can configure VRRP text authentication, authentication using a simple MD5 key string, or MD5 key chains for authentication.

MD5 authentication provides greater security than the alternative plain text authentication scheme. MD5 authentication allows each VRRP group member to use a secret key to generate a keyed MD5 hash of the packet that is part of the outgoing packet. A keyed hash of an incoming packet is generated and if the generated hash does not match the hash within the incoming packet, the packet is ignored.

The key for the MD5 hash can either be given directly in the configuration using a key string or supplied indirectly through a key chain.

A router ignores incoming VRRP packets from routers that do not have the same authentication configuration for a VRRP group. VRRP has three authentication schemes:

- No authentication
- Plain text authentication
- MD5 authentication

VRRP packets are rejected in any of the following cases:

- The authentication schemes differ on the router and in the incoming packet.
- MD5 digests differ on the router and in the incoming packet.
- Text authentication strings differ on the router and in the incoming packet.

ISSU—VRRP

VRRP supports In Service Software Upgrade (ISSU). An ISSU allows a high-availability (HA) system to run in Stateful Switchover (SSO) mode even when different versions of Cisco IOS software are running on the active and standby Route Processors (RPs) or line cards.

ISSU provides the ability to upgrade or downgrade from one supported Cisco IOS release to another while continuing to forward packets and maintain sessions, thereby reducing planned outage time. The ability to upgrade or downgrade is achieved by running different software versions on the active RP and standby RP for a short period of time to maintain state information between RPs. This feature allows the system to switch over to a secondary RP running upgraded (or downgraded) software and continue forwarding packets without session loss and with minimal or no packet loss. This feature is enabled by default.

For detailed information about ISSU, see the Cisco IOS In Service Software Upgrade Process document at the following URL:


For detailed information about ISSU on the 7600 series routers, see the ISSU and eFSU on Cisco 7600 Series Routers document at the following URL:

SSO—VRRP

With the introduction of the SSO—VRRP feature, VRRP is SSO aware. VRRP can detect when a router is failing over to the secondary RP and continue in its current group state.

SSO functions in networking devices (usually edge devices) that support dual Route Processors (RPs). SSO provides RP redundancy by establishing one of the RPs as the active processor and the other RP as the standby processor. SSO also synchronizes critical state information between the RPs so that network state information is dynamically maintained between RPs.

Prior to being SSO aware, if VRRP was deployed on a router with redundant RPs, a switchover of roles between the active RP and the standby RP would result in the router relinquishing its activity as a VRRP group member and then rejoining the group as if it had been reloaded. The SSO—VRRP feature enables VRRP to continue its activities as a group member during a switchover. VRRP state information between redundant RPs is maintained so that the standby RP can continue the router’s activities within the VRRP during and after a switchover.

This feature is enabled by default. To disable this feature, use the `no vrrp sso` command in global configuration mode.

For more information, see the Stateful Switchover document at the following URL:


Configuring VRRP

The following sections outline the steps necessary to configure VRRP:

- Customizing VRRP, page 31-7 (optional)
- Enabling VRRP, page 31-8 (required)
- Disabling VRRP on an Interface, page 31-9 (optional)
- Configuring VRRP Object Tracking, page 31-10 (optional)
- Configuring VRRP MD5 Authentication Using a Key String, page 31-11 (optional)
- Configuring VRRP MD5 Authentication Using a Key Chain, page 31-12 (optional)
- Verifying the VRRP MD5 Authentication Configuration, page 31-13 (optional)
- Configuring VRRP Text Authentication, page 31-14 (optional)
- Enabling the Router to Send SNMP VRRP Notifications, page 31-15 (optional)

Customizing VRRP

Customizing the behavior of VRRP is optional. Be aware that as soon as you enable a VRRP group, that group is operating. It is possible that if you first enable a VRRP group before customizing VRRP, the router could take over control of the group and become the virtual router master before you have finished customizing the feature. Therefore, if you plan to customize VRRP, it is a good idea to do so before enabling VRRP.

Complete the following steps in privileged EXEC mode to customize VRRP:
### Configuring VRRP

#### Enabling VRRP

To enable VRRP perform the following steps.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3 interface type number</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>Step 4 ip address ip-address mask</td>
<td>Configures an IP address for an interface.</td>
</tr>
<tr>
<td>Step 5 vrrp group description text</td>
<td>Assigns a text description to the VRRP group.</td>
</tr>
<tr>
<td>Step 6 vrrp group priority level</td>
<td>Sets the priority level of the router within a VRRP group.</td>
</tr>
<tr>
<td>Step 7 vrrp group preempt [delay minimum seconds]</td>
<td>Configures the router to take over as virtual router master for a VRRP group if it has a higher priority than the current virtual router master.</td>
</tr>
<tr>
<td>Step 8 vrrp group timers advertise [msec] interval</td>
<td>Configures the interval between successive advertisements by the virtual router master in a VRRP group.</td>
</tr>
<tr>
<td>Step 9 vrrp group timers learn</td>
<td>Configures the router, when it is acting as virtual router backup for a VRRP group, to learn the advertisement interval used by the virtual router master.</td>
</tr>
<tr>
<td>Step 10 no vrrp sso</td>
<td>(Optional) Disables VRRP support of SSO. VRRP support of SSO is enabled by default.</td>
</tr>
</tbody>
</table>

### Note

All routers in a VRRP group must use the same timer values. If the same timer values are not set, the routers in the VRRP group will not communicate with each other and any misconfigured router will change its state to master.
### Configuring VRRP

Disabling VRRP on an Interface

Disabling VRRP on an interface allows the protocol to be disabled, but the configuration retained. This ability was added with the introduction of the VRRP MIB, RFC 2787, Definitions of Managed Objects for the Virtual Router Redundancy Protocol.

You can use a Simple Network Management Protocol (SNMP) management tool to enable or disable VRRP on an interface. Because of the SNMP management capability, the `vrrp shutdown` command was introduced to represent a method via the CLI for VRRP to show the state that had been configured using SNMP.

When the `show running-config` command is entered, you can see immediately if the VRRP group has been configured and set to enabled or disabled. This is the same functionality that is enabled within the MIB.

The `no` form of the command enables the same operation that is performed within the MIB. If the `vrrp shutdown` command is specified using the SNMP interface, then entering the `no vrrp shutdown` command using the Cisco IOS CLI will reenable the VRRP group.

To disable VRRP perform the following steps.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

### Disabling VRRP on an Interface

Disabling VRRP on an interface allows the protocol to be disabled, but the configuration retained. This ability was added with the introduction of the VRRP MIB, RFC 2787, Definitions of Managed Objects for the Virtual Router Redundancy Protocol.

You can use a Simple Network Management Protocol (SNMP) management tool to enable or disable VRRP on an interface. Because of the SNMP management capability, the `vrrp shutdown` command was introduced to represent a method via the CLI for VRRP to show the state that had been configured using SNMP.

When the `show running-config` command is entered, you can see immediately if the VRRP group has been configured and set to enabled or disabled. This is the same functionality that is enabled within the MIB.

The `no` form of the command enables the same operation that is performed within the MIB. If the `vrrp shutdown` command is specified using the SNMP interface, then entering the `no vrrp shutdown` command using the Cisco IOS CLI will reenable the VRRP group.

To disable VRRP perform the following steps.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

### Disabling VRRP on an Interface

Disabling VRRP on an interface allows the protocol to be disabled, but the configuration retained. This ability was added with the introduction of the VRRP MIB, RFC 2787, Definitions of Managed Objects for the Virtual Router Redundancy Protocol.

You can use a Simple Network Management Protocol (SNMP) management tool to enable or disable VRRP on an interface. Because of the SNMP management capability, the `vrrp shutdown` command was introduced to represent a method via the CLI for VRRP to show the state that had been configured using SNMP.

When the `show running-config` command is entered, you can see immediately if the VRRP group has been configured and set to enabled or disabled. This is the same functionality that is enabled within the MIB.

The `no` form of the command enables the same operation that is performed within the MIB. If the `vrrp shutdown` command is specified using the SNMP interface, then entering the `no vrrp shutdown` command using the Cisco IOS CLI will reenable the VRRP group.

To disable VRRP perform the following steps.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
### Configuring VRRP

#### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td><code>interface type number</code></td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>3.2</td>
<td><code>ip address ip-address mask</code></td>
<td>Configures an IP address for an interface.</td>
</tr>
<tr>
<td>3.3</td>
<td><code>vrrp group shutdown</code></td>
<td>Disables VRRP on an interface.</td>
</tr>
</tbody>
</table>

*Note*  
You can have one VRRP group disabled, while retaining its configuration, and a different VRRP group enabled.

### Configuring VRRP Object Tracking

#### Restrictions

The following restriction applies to VRRP object tracking.

If a VRRP group is the IP address owner, its priority is fixed at 255 and cannot be reduced through object tracking.

To configure VRRP object tracking perform the following steps.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 3.1  | `enable`                                                                          | Enables privileged EXEC mode.  
|                                                |   - Enter your password if prompted.                                                              |
| 3.2  | `configure terminal`                                                             | Enters global configuration mode.                                                                  |
| 3.3  | `track object-number interface type number {line-protocol | ip routing}`                 | Configures an interface to be tracked where changes in the state of the interface affect the priority of a VRRP group.  
|                                                |   - This command configures the interface and corresponding object number to be used with the `vrrp track` command.  
|                                                |   - The `line-protocol` keyword tracks whether the interface is up. The `ip routing` keyword also checks that IP routing is enabled and active on the interface.  
|                                                |   - You can also use the `track ip route` command to track the reachability of an IP route or a metric type object.  |
| 3.4  | `interface type number`                                                          | Enters interface configuration mode.                                                                |
| 3.5  | `vrrp group ip ip-address`                                                        | Enables VRRP on an interface and identifies the IP address of the virtual router.                  |
| 3.6  | `vrrp group priority level`                                                       | Sets the priority level of the router within a VRRP group.                                          |
| 3.7  | `vrrp group track object-number [decrement priority]`                            | Configures VRRP to track an object.                                                                 |
Chapter 31 Configuring Virtual Router Redundancy Protocol

Configuring VRRP MD5 Authentication Using a Key String

Restrictions

The following restrictions apply to configuring VRRP MD5 Authentication using a key string.

- Interoperability with vendors that may have implemented the RFC 2338 method is not enabled.
- Text authentication cannot be combined with MD5 authentication for a VRRP group at any one time. When MD5 authentication is configured, the text authentication field in VRRP hello messages is set to all zeroes on transmit and ignored on receipt, provided the receiving router also has MD5 authentication enabled.

To configure VRRP MD5 Authentication using a key string perform the following steps.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 8 end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 9 show track [object-number]</td>
<td>Displays tracking information.</td>
</tr>
</tbody>
</table>

Command or Action | Purpose |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3 interface type number</td>
<td>Configures an interface type and enters interface configuration mode.</td>
</tr>
<tr>
<td>Step 4 ip address ip-address mask [secondary]</td>
<td>Specifies a primary or secondary IP address for an interface.</td>
</tr>
<tr>
<td>Step 5 vrrp group priority priority</td>
<td>Configures VRRP priority.</td>
</tr>
</tbody>
</table>
Configuring VRRP MD5 Authentication Using a Key Chain

Perform this task to configure VRRP MD5 authentication using a key chain. Key chains allow a different key string to be used at different times according to the key chain configuration. VRRP will query the appropriate key chain to obtain the current live key and key ID for the specified key chain.

Restrictions

The following restrictions apply to configuring VRRP MD5 using a keychain.

- Interoperability with vendors that may have implemented the RFC 2338 method is not enabled.
- Text authentication cannot be combined with MD5 authentication for a VRRP group at any one time. When MD5 authentication is configured, the text authentication field in VRRP hello messages is set to all zeroes on transmit and ignored on receipt, provided the receiving router also has MD5 authentication enabled.

To configure VRRP MD5 authentication using a key chain perform the following steps.
### Configuring VRRP

#### Verifying the VRRP MD5 Authentication Configuration

To verify the VRRP MD5 authentication configuration perform the following steps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> key chain name-of-chain</td>
<td>Enables authentication for routing protocols and identifies a group of authentication keys.</td>
</tr>
<tr>
<td><strong>Step 4</strong> key key-id</td>
<td>Identifies an authentication key on a key chain.</td>
</tr>
<tr>
<td></td>
<td>• The key-id must be a number.</td>
</tr>
<tr>
<td><strong>Step 5</strong> key-string string</td>
<td>Specifies the authentication string for a key.</td>
</tr>
<tr>
<td></td>
<td>• The string can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a number.</td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong> interface type number</td>
<td>Configures an interface type and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 8</strong> ip address ip-address mask [secondary]</td>
<td>Specifies a primary or secondary IP address for an interface.</td>
</tr>
<tr>
<td><strong>Step 9</strong> vrrp group priority priority</td>
<td>Configures VRRP priority.</td>
</tr>
<tr>
<td><strong>Step 10</strong> vrrp group authentication md5 key-chain key-chain</td>
<td>Configures an authentication MD5 key chain for VRRP MD5 authentication.</td>
</tr>
<tr>
<td></td>
<td>• The key chain name must match the name specified in Step 3.</td>
</tr>
<tr>
<td></td>
<td>Note: All routers within the VRRP group must be configured with the same authentication string. If the same authentication string is not configured, the routers in the VRRP group will not communicate with each other and any misconfigured router will change its state to master.</td>
</tr>
<tr>
<td><strong>Step 11</strong> vrrp group ip [ip-address [secondary]]</td>
<td>Enables VRRP on an interface and identifies the IP address of the virtual router.</td>
</tr>
<tr>
<td><strong>Step 12</strong> Repeat Steps 1 through 11 on each router that will communicate.</td>
<td>—</td>
</tr>
<tr>
<td><strong>Step 13</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Configuring VRRP

#### Step 1  show vrrp

Use this command to verify that the authentication is configured correctly:

```
Router# show vrrp
```

```
Ethernet0/1 - Group 1
State is Master
Virtual IP address is 10.21.0.10
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 1.000 sec
Preemption is enabled
  min delay is 0.000 sec
Priority is 100
  Authentication MD5, key-string, timeout 30 secs
Master Router is 10.21.0.1 (local), priority is 100
Master Advertisement interval is 1.000 sec
Master Down interval is 3.609 sec
```

This output shows that MD5 authentication is configured and the f00d4s key string is used. The timeout value is set at 30 seconds.

#### Step 2  debug vrrp authentication

Use this command to verify that both routers have authentication configured, that the MD5 key ID is the same on each router, and that the MD5 key strings are the same on each router:

```
Router1#: debug vrrp authentication
```

```
VRRP: Sent: 21016401FE0500000AC1801FE0000000000000000
VRRP: HshC: B861CBF1B9026130DD34AED849BEC8A1
VRRP: Rcvd: 21016401FE0500000AC1801FE0000000000000000
VRRP: HshC: B861CBF1B9026130DD34AED849BEC8A1
VRRP: HshR: C5E193C6D84533FDC750F85FCFB051E1
VRRP: Grp 1 Adv from 172.24.1.2 has failed MD5 auth
```

```
Router2#: debug vrrp authentication
```

```
VRRP: Sent: 21016401FE0500000AC1801FE0000000000000000
VRRP: HshC: C5E193C6D84533FDC750F85FCFB051E1
VRRP: Rcvd: 21016401FE0500000AC1801FE0000000000000000
VRRP: HshC: C5E193C6D84533FDC750F85FCFB051E1
VRRP: HshR: B861CBF1B9026130DD34AED849BEC8A1
VRRP: Grp 1 Adv from 172.24.1.1 has failed MD5 auth
```

---

### Configuring VRRP Text Authentication

#### Restrictions

The following restrictions apply to configuring VRRP text authentication:

- Interoperability with vendors that may have implemented the RFC 2338 method is not enabled.
- Text authentication cannot be combined with MD5 authentication for a VRRP group at any one time. When MD5 authentication is configured, the text authentication field in VRRP hello messages is set to all zeroes on transmit and ignored on receipt, provided the receiving router also has MD5 authentication enabled.
To configure VRRP text authentication perform the following steps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables higher privilege levels, such as privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3 interface type number</td>
<td>Configures an interface type and enters interface configuration mode.</td>
</tr>
<tr>
<td>Step 4 ip address ip-address mask [secondary]</td>
<td>Specifies a primary or secondary IP address for an interface.</td>
</tr>
<tr>
<td>Step 5 vrrp group authentication text text-string</td>
<td>Authenticates VRRP packets received from other routers in the group.</td>
</tr>
<tr>
<td>Step 6 vrrp group ip ip-address</td>
<td>Enables VRRP on an interface and identifies the IP address of the virtual router.</td>
</tr>
<tr>
<td>Step 7 Repeat Steps 1 through 6 on each router that will communicate.</td>
<td>—</td>
</tr>
<tr>
<td>Step 8 end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

**Note** All routers within the VRRP group must be configured with the same authentication string. If the same authentication string is not configured, the routers in the VRRP group will not communicate with each other and any misconfigured router will change its state to master.

**Enabling the Router to Send SNMP VRRP Notifications**

The VRRP MIB supports SNMP Get operations, which allow network devices to get reports about VRRP groups in a network from the network management station.

Enabling VRRP MIB trap support is performed through the CLI, and the MIB is used for collecting reports. A trap notifies the network management station when a router becomes a Master or backup router. When an entry is configured from the CLI, the RowStatus for that group in the MIB immediately goes to the active state.

To enable the router to send SNMP VRRP notifications perform the following steps:
Command or Action | Purpose
---|---
Step 1 | enable
| Enables privileged EXEC mode.
| Enter your password if prompted.
Step 2 | configure terminal
| Enters global configuration mode.
Step 3 | snmp-server enable traps vrrp
| Enables the router to send SNMP VRRP notifications (traps and informs).
Step 4 | snmp-server host host community-string vrrp
| Specifies the recipient of an SNMP notification operation.

Configuration Examples for VRRP

- Example: Configuring VRRP, page 31-16
- Example: VRRP Object Tracking, page 31-17
- Example: VRRP Object Tracking Verification, page 31-17
- Example: VRRP MD5 Authentication Configuration Using a Key String, page 31-18
- Example: VRRP MD5 Authentication Configuration Using a Key Chain, page 31-18
- Example: VRRP Text Authentication, page 31-18
- Example: Disabling a VRRP Group on an Interface, page 31-19
- Example: VRRP MIB Trap, page 31-19

Example: Configuring VRRP

In the following example, Router A and Router B each belong to three VRRP groups.
In the configuration, each group has the following properties:

- Group 1:
  - Virtual IP address is 10.1.0.10.
  - Router A will become the master for this group with priority 120.
  - Advertising interval is 3 seconds.
  - Preemption is enabled.
- Group 5:
  - Router B will become the master for this group with priority 200.
  - Advertising interval is 30 seconds.
  - Preemption is enabled.
- Group 100:
  - Router A will become the master for this group first because it has a higher IP address (10.1.0.2).
  - Advertising interval is the default 1 second.
  - Preemption is disabled.
**Router A**

RouterA(config)# interface ethernet 1/0
RouterA(config-if)# ip address 10.1.0.2 255.0.0.0
RouterA(config-if)# vrrp 1 priority 120
RouterA(config-if)# vrrp 1 authentication cisco
RouterA(config-if)# vrrp 1 timers advertise 3
RouterA(config-if)# vrrp 1 timers learn
RouterA(config-if)# vrrp 1 ip 10.1.0.10
RouterA(config-if)# vrrp 5 priority 100
RouterA(config-if)# vrrp 5 timers advertise 30
RouterA(config-if)# vrrp 5 timers learn
RouterA(config-if)# vrrp 5 ip 10.1.0.50
RouterA(config-if)# vrrp 100 timers learn
RouterA(config-if)# no vrrp 100 preempt
RouterA(config-if)# vrrp 100 ip 10.1.0.100
RouterA(config-if)# no shutdown

**Router B**

RouterB(config)# interface ethernet 1/0
RouterB(config-if)# ip address 10.1.0.1 255.0.0.0
RouterB(config-if)# vrrp 1 priority 100
RouterB(config-if)# vrrp 1 authentication cisco
RouterB(config-if)# vrrp 1 timers advertise 3
RouterB(config-if)# vrrp 1 timers learn
RouterB(config-if)# vrrp 1 ip 10.1.0.10
RouterB(config-if)# vrrp 5 priority 200
RouterB(config-if)# vrrp 5 timers advertise 30
RouterB(config-if)# vrrp 5 timers learn
RouterB(config-if)# vrrp 5 ip 10.1.0.50
RouterB(config-if)# vrrp 100 timers learn
RouterB(config-if)# no vrrp 100 preempt
RouterB(config-if)# vrrp 100 ip 10.1.0.100
RouterB(config-if)# no shutdown

**Example: VRRP Object Tracking**

In the following example, the tracking process is configured to track the state of the line protocol on serial interface 0/1. VRRP on Ethernet interface 1/0 then registers with the tracking process to be informed of any changes to the line protocol state of serial interface 0/1. If the line protocol state on serial interface 0/1 goes down, then the priority of the VRRP group is reduced by 15.

Router(config)# track 1 interface Serial0/1 line-protocol
Router(config-track)# exit
Router(config)# interface Ethernet1/0
Router(config-if)# ip address 10.0.0.2 255.0.0.0
Router(config-if)# vrrp 1 ip 10.0.0.3
Router(config-if)# vrrp 1 priority 120
Router(config-if)# vrrp 1 track 1 decrement 15

**Example: VRRP Object Tracking Verification**

The following examples verify the configuration shown in the “Example: VRRP Object Tracking” section:

Router# show vrrp

Ethernet1/0 - Group 1
  State is Master
Virtual IP address is 10.0.0.3
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 1.000 sec
Preemption is enabled
min delay is 0.000 sec
Priority is 105
Track object 1 state Down decrement 15
Master Router is 10.0.0.2 (local), priority is 105
Master Advertisement interval is 1.000 sec
Master Down interval is 3.531 sec

Router# show track

Track 1
  Interface Serial0/1 line-protocol
  Line protocol is Down (hw down)
  1 change, last change 00:06:53
  Tracked by:
    VRRP Ethernet1/0 1

Example: VRRP MD5 Authentication Configuration Using a Key String

The following example shows how to configure MD5 authentication using a key string and timeout of
30 seconds:

Router(config)# interface Ethernet0/1
Router(config-if)# description ed1-cat5a-7/10
Router(config-if)# vrrp 1 ip 10.21.0.10
Router(config-if)# vrrp 1 priority 110
Router(config-if)# vrrp 1 authentication md5 key-string f00c4s timeout 30
Router(config-if)#

Example: VRRP MD5 Authentication Configuration Using a Key Chain

The following example shows how to configure MD5 authentication using a key chain:

Router(config)# key chain vrrp1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string f00c4s
Router(config-keychain-key)# exit
Router(config)# interface ethernet0/1
Router(config-if)# description ed1-cat5a-7/10
Router(config-if)# vrrp 1 priority 110
Router(config-if)# vrrp 1 authentication md5 key-chain vrrp1
Router(config-if)# vrrp 1 ip 10.21.0.10

In this example, VRRP queries the key chain to obtain the current live key and key ID for the specified
key chain.

Example: VRRP Text Authentication

The following example shows how to configure VRRP text authentication using a text string:

Router(config)# interface fastethernet 0/0
Router(config-if)# ip address 10.21.8.32 255.255.255.0
Router(config-if)# vrrp 10 authentication text stringxyz
Router(config-if)# vrrp 10 ip 10.21.8.10
Example: Disabling a VRRP Group on an Interface

The following example shows how to disable one VRRP group on Ethernet interface 0/1 while retaining VRRP for group 2 on Ethernet interface 0/2:

```
Router(config)# interface ethernet0/1
Router(config-if)# ip address 10.24.1.1 255.255.255.0
Router(config-if)# vrrp 1 ip 10.24.1.254
Router(config-if)# vrrp 1 shutdown
Router(config-if)# exit
Router(config)# interface ethernet0/2
Router(config-if)# ip address 10.168.42.1 255.255.255.0
Router(config-if)# vrrp 2 ip 10.168.42.254
```

Example: VRRP MIB Trap

The following example shows how to enable the VRRP MIB trap support functionality:

```
Router(config)# snmp-server enable traps vrrp
Router(config)# snmp-server host 10.1.1.0 community abc vrrp
```
Configuring HSRP

This chapter describes how to use Hot Standby Router Protocol (HSRP) on the Cisco ME 3800X and ME 3600X switch to provide routing redundancy for routing IP traffic without being dependent on the availability of any single router.

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 IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2.

- Understanding HSRP, page 32-1
- Configuring HSRP, page 32-3
- Displaying HSRP Configurations, page 32-9

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 routed ports and switch virtual interfaces (SVIs) on the switch.

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.
Chapter 32 Configuring HSRP

Understanding HSRP

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 disabled by default 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 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 32-1 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

The switch supports 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.

### Configuring HSRP

- Default HSRP Configuration, page 32-4
- Restrictions and Guidelines, page 32-4
- Enabling HSRP, page 32-5
- Configuring HSRP Priority, page 32-6
- Configuring HSRP Authentication and Timers, page 32-8
• Enabling HSRP Support for ICMP Redirect Messages, page 32-9

Default HSRP Configuration

Table 32-1 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>

Restrictions and Guidelines

The following restrictions apply to HSRP:

- There are 128 HSRP groups supported on the ME3600x device and 256 HSRP groups supported on a ME3800x device.
- Both the ME3600 and ME3800 devices support up to 4 groups per VLAN or routing interface.
- In the 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 28-12.
- All Layer 3 interfaces must have IP addresses assigned to them. See the “Configuring Layer 3 Interfaces” section on page 10-19.
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.

Complete these steps in privileged EXEC mode, to create or enable HSRP on a Layer 3 interface:

<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 interface configuration mode, and enter the Layer 3 interface on which you want to enable HSRP.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>no switchport</code> If necessary, disable Layer 2 switching on the port to enable the Layer 3 interface.</td>
</tr>
<tr>
<td>Step 4</td>
<td>`standby version {1</td>
</tr>
<tr>
<td></td>
<td>• 1— Select HSRPv1.</td>
</tr>
<tr>
<td></td>
<td>• 2— Select HSRPv2. (Not supported on ME3600/ME3800 switch.)</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> While the command exists to change the HSRP version, it is not applicable on the ME3600/ME3800 because only default HSRP version 1 is supported.</td>
</tr>
<tr>
<td></td>
<td>If you do not enter this command or do not specify a keyword, the interface runs the default HSRP version, that is version 1.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>standby [group-number] ip [ip-address [secondary]]</code> Create (or enable) the HSRP group using its number and virtual IP address.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) <code>group-number</code>—The 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) <code>ip-address</code>—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) <code>secondary</code>—The IP address is a secondary hot standby router interface. If neither router is designated as a secondary or standby router and no priorities are set, the primary IP addresses are compared and the higher IP address is the active router, with the next highest as the standby router.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>show standby [interface-id [group]]</code> Verify the configuration.</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>
Use the `no standby [group-number] ip [ip-address]` 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.

This procedure is the minimum number of steps required to enable HSRP. Other configuration is optional.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# end
Switch# show standby
```

### Configuring HSRP Priority

The `standby priority`, `standby preempt`, and `standby track` interface configuration commands are all used to set characteristics for finding active and standby routers and behavior regarding when a new active router takes over.

When configuring HSRP 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>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 HSRP interface on which you want to set priority.</td>
</tr>
</tbody>
</table>
| 3    | standby [group-number] priority priority [preempt [delay delay]] | Set a priority value used in choosing the active router. The range is 1 to 255; the default priority is 100. The highest number represents the highest priority.  
  - (Optional) group-number—The group number to which the command applies.  
  - (Optional) preempt—Select so that when the local router has a higher priority than the active router, it assumes control as the active router.  
  - (Optional) delay—Set to cause the local router to postpone taking over the active role for the shown number of seconds. The range is 0 to 3600 (1 hour); the default is 0 (no delay before taking over).  
  Use the no form of the command to restore the default values. |
| 4    | standby [group-number] [priority priority] preempt [delay delay] | Configure the router to preempt, which means that when the local router has a higher priority than the active router, it assumes control as the active router.  
  - (Optional) group-number—The group number to which the command applies.  
  - (Optional) priority—Enter to set or change the group priority. The range is 1 to 255; the default is 100.  
  - (Optional) delay—Set to cause the local router to postpone taking over the active role for the number of seconds shown. The range is 0 to 3600 (1 hour); the default is 0 (no delay before taking over).  
  Use the no form of the command to restore the default values. |
| 5    | standby [group-number] track type number [interface-priority] | 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.  
  - (Optional) group-number—The group number to which the command applies.  
  - type—Enter the interface type (combined with interface number) that is tracked.  
  - number—Enter the interface number (combined with interface type) that is tracked.  
  - (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. |
| 6    | end | Return to privileged EXEC mode. |
| 7    | show running-config | Verify the configuration of the standby groups. |
| 8    | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

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.
Chapter 32      Configuring HSRP

Configuring HSRP

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:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# standby ip 172.20.128.3
Switch(config-if)# standby priority 120 preempt delay 300
Switch(config-if)# end
```

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 hellotime.

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</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>Enter interface configuration mode, and enter the HSRP interface</td>
</tr>
<tr>
<td></td>
<td>on which you want to set authentication.</td>
</tr>
<tr>
<td>Step 3</td>
<td></td>
</tr>
<tr>
<td>standby [group-number] authentication string</td>
<td>(Optional) <strong>authentication string</strong>—Enter a string to be carried in</td>
</tr>
<tr>
<td></td>
<td>all HSRP messages. The authentication string can be up to eight</td>
</tr>
<tr>
<td></td>
<td>characters in length; the default string is <strong>cisco</strong>.</td>
</tr>
<tr>
<td></td>
<td>(Optional) <strong>group-number</strong>—The group number to which the</td>
</tr>
<tr>
<td></td>
<td>command applies.</td>
</tr>
<tr>
<td>Step 4</td>
<td></td>
</tr>
<tr>
<td>standby [group-number] timers hellotime holdtime</td>
<td>(Optional) Configure the time between hello packets and the time</td>
</tr>
<tr>
<td></td>
<td>before other routers declare the active router to be down.</td>
</tr>
<tr>
<td></td>
<td>- <strong>group-number</strong>—The group number to which the command</td>
</tr>
<tr>
<td></td>
<td>applies.</td>
</tr>
<tr>
<td></td>
<td>- <strong>hellotime</strong>—The hello interval in seconds. The range is from 1</td>
</tr>
<tr>
<td></td>
<td>to 255; the default is 3 seconds.</td>
</tr>
<tr>
<td></td>
<td>- <strong>holdtime</strong>—The time in seconds before the active or standby</td>
</tr>
<tr>
<td></td>
<td>router is declared to be down. The range is from 1 to 255; the</td>
</tr>
<tr>
<td></td>
<td>default is 10 seconds.</td>
</tr>
</tbody>
</table>

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:
### Displaying HSRP Configurations

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6 show running-config</td>
<td>Verify the configuration of the standby groups.</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 standby [group-number] authentication string` interface configuration command to delete an authentication string. Use the `no standby [group-number] timers hello-time hold-time` 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:

```plaintext
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 authentication word
Switch(config-if)# end
```

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:

```plaintext
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# standby 1 timers 5 15
Switch(config-if)# end
```

### 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 172.20.128.3 configured
  Active router is 172.20.128.1 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
  Hellotime 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) on the Cisco ME 3800X and 3600X 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.

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 33-1
- Configuring IP SLAs Operations, page 33-6
- Monitoring IP SLAs Operations, page 33-12

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 33-2
- IP SLAs Responder and IP SLAs Control Protocol, page 33-3
- Response Time Computation for IP SLAs, page 33-4
- IP SLAs Operation Scheduling, page 33-5
- IP SLAs Operation Threshold Monitoring, page 33-5

**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 33-1 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.

Figure 33-1 Cisco IOS IP SLAs Operation

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 IP SLAs 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.
The IP SLAs responder can be a Cisco IOS Layer 2, responder-configurable switch, such as a Catalyst 2960 or Cisco ME 2400 switch or a Cisco ME 3400 switch running the metro base image. The responder does not need to support full IP SLAs functionality.

Figure 33-1 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 33-2 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 includes 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 33-6
- Configuration Guidelines, page 33-6
- Configuring the IP SLAs Responder, page 33-7
- Analyzing IP Service Levels by Using the UDP Jitter Operation, page 33-8
- Analyzing IP Service Levels by Using the ICMP Echo Operation, page 33-10

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 IP SLAs 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 or a Cisco ME 3400 switch running the metro base image. 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>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip sla responder {tcp-connect</td>
</tr>
<tr>
<td>Note</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>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ip sla responder</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

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.

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>
</tbody>
</table>
### Step 3
```
udp-jitter {destination-ip-address \ destination-hostname} destination-port [source-ip {ip-address \ hostname}] [source-port port-number] [control {enable \ disable}] [num-packets number-of-packets] [interval interpacket-interval]
```
Configure the IP SLAs operation as a UDP jitter operation, and enter UDP jitter configuration mode.

- `destination-ip-address \ destination-hostname`—Specify the destination IP address or hostname.
- `destination-port`—Specify the destination port number in the range from 1 to 65535.
- (Optional) `source-ip {ip-address \ 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.
- (Optional) `source-port port-number`—Specify the source port number in the range from 1 to 65535. When a port number is not specified, IP SLAs chooses an available port.
- (Optional) `control {enable \ disable}`—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.
- (Optional) `num-packets number-of-packets`—Enter the number of packets to be generated. The range is 1 to 6000; the default is 10.
- (Optional) `interval interpacket-interval`—Enter the interval between sending packets in milliseconds. The range is 1 to 6000; the default value is 20 ms.

### Step 4
```
frequency seconds
```
(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.

### Step 5
```
exit
```
Exit UDP jitter configuration mode, and return to global configuration mode.

### Step 6
```
ip sla monitor schedule operation-number [life {forever \ seconds}] [start-time {hh:mm [:ss] \ month day \ day month} | pending \ now | after hh:mm:ss] [ageout seconds] [recurring]
```
Configure the scheduling configuration parameters for an individual IP SLAs operation.

- `operation-number`—Enter the RTR entry number.
- (Optional) `life {forever \ seconds}`—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) `start-time {hh:mm [:ss] \ month day \ day month} | pending \ now | after hh:mm:ss`—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 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.
- (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).
- (Optional) `recurring`—Set the operation to automatically run every day.
Configuring IP SLAs Operations

### Chapter 33      Configuring Cisco IOS IP SLAs Operations

#### Command

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>8</td>
<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>
<tr>
<td>9</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 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:

```plaintext
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

Entry number: 10
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>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>ip sla operation-number</strong></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><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</td>
</tr>
<tr>
<td></td>
<td>• (Optional) source-interface interface-id—Specify the source interface for the operation.</td>
</tr>
<tr>
<td><strong>Step 4</strong></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><strong>Step 5</strong></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><strong>Step 6</strong></td>
<td>**ip sla schedule operation-number [life</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><strong>Step 7</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</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 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
Switch(config)# end
Switch# show ip sla configuration 22
IP SLAs, Infrastructure Engine-II.
Entry number: 12
Owner:
Tag:
Type of operation to perform: echo
Target address: 2.2.2.2
Source address: 0.0.0.0
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Schedule:
    Operation frequency (seconds): 60
    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
History Statistics:
    Number of history Lives kept: 0
    Number of history Buckets kept: 15
    History Filter Type: None
Enhanced History:
```

**Monitoring IP SLAs Operations**

Use the User EXEC or Privileged EXEC commands in Table 33-1 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 configuration</td>
<td>Display IP SLAs authentication information.</td>
</tr>
<tr>
<td>show ip sla configuration</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</td>
<td>Display enhanced history statistics for collected history buckets or distribution statistics for all IP SLAs operations or a specific operation.</td>
</tr>
<tr>
<td>show ip sla ethernet-monitor configuration</td>
<td>Display IP SLAs automatic Ethernet configuration.</td>
</tr>
<tr>
<td>show ip sla group schedule</td>
<td>Display IP SLAs group scheduling configuration and details.</td>
</tr>
<tr>
<td>show ip sla history</td>
<td>Display history collected for all IP SLAs operations.</td>
</tr>
<tr>
<td>show ip sla mpls-lsp-monitor</td>
<td>Display MPLS label switched path (LSP) Health Monitor operations,</td>
</tr>
<tr>
<td>show ip sla reaction-configuration</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</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</td>
<td>Display current or aggregated operational status and statistics.</td>
</tr>
</tbody>
</table>
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 Cisco ME 3800X and ME 3600X 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.

This chapter provides information about configuring CFM, E-LMI, and the Ethernet OAM protocol.

For complete command and configuration information for Ethernet OAM, CFM, and E-LMI, see the Cisco IOS Carrier Ethernet Configuration Guide at this URL: http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/12_2sr/ce_12_2sr_book.html

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: http://www.cisco.com/en/US/docs/ios/cether/command/reference/ce_book.html

This chapter contains these sections:

- Understanding Ethernet CFM, page 34-1
- Configuring Ethernet CFM, page 34-7
- Managing and Displaying Ethernet CFM Information, page 34-23
- Understanding the Ethernet OAM Protocol, page 34-25
- Setting Up and Configuring Ethernet OAM, page 34-27
- Displaying Ethernet OAM Protocol Information, page 34-35
- Understanding E-LMI, page 34-35
- Configuring E-LMI, page 34-36
- Displaying E-LMI, page 34-38
- Ethernet CFM and Ethernet OAM Interaction, page 34-38

**Understanding Ethernet CFM**

Ethernet CFM is an end-to-end 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.
The switch does not support:

- CFM on VFI interfaces
- Provider-edge E-LMI
- CFM on bridge domains (supported on switchports only)
- CFM on SVI based xconnect
- CFM on port based xconnect

Note

CFM is supported on EVC BD, EVC xconnect, EFP xconnect and CFM transparencys.

These sections contain conceptual information about Ethernet CFM:

- CFM Domain, page 34-2
- Maintenance Associations and Maintenance Points, page 34-3
- CFM Messages, page 34-4
- Crosscheck Function and Static Remote MEPs, page 34-5
- SNMP Traps and Fault Alarms, page 34-5
- Configuration Error List, page 34-5
- IP SLAs Support for CFM, page 34-6
- CFM on EVC Bridge Domains and EVC Cross-Connect Interfaces, page 34-6

**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 34-1, 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 34-2, 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 contracts 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 administering organizations. CFM exchanges messages and performs operations on a per-domain basis.
Understanding Ethernet CFM

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.
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 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.

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.

**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 one time 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. 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.
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 33, “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.

For more information about IP SLAs operation with CFM, see the IP SLAs for Metro-Ethernet feature module at this URL:


CFM on EVC Bridge Domains and EVC Cross-Connect Interfaces

CFM is supported on EVC bridge domains and EVC cross-connect interfaces. EVC interfaces can be used to connect UNI interfaces so that VLAN IDs can be mapped to bridge domains.

CFM is supported on the following types of EVCs:

- Default
- Tagged
- Untagged
- Single-dot1q tagged
- QinQ

CFM over pseudowires allows service providers to manage access-side, end-to-end connectivity over an MPLS core.

CFM packets can be forwarded over:

- SVI Pseudo-wire
- VPLS Pseudo-wire
- EVC Xconnect Pseudo-wire
- Bridge-domain
- VLAN

The following CFM features are supported on the Cisco ME3600/ME3800 switches:

- CFM transparency on SVI PW / VPLS PW / EVC xconnect PW
- CFM Up MEP on EVC Xconnect and Port-Channel EVC Xconnect
- CFM Down MEP on EVC BD and Port-Channel EVC Xconnect
- CFM Up MEP on EVC BD and Port-Channel EVC Xconnect
- MIP support
- CFM IEEE MIB (EVC BD, EVC Xconnect)
- ELMI PE and CE support
- CFM ELMI Interworking
- CFM and 802.3ah interworking
- SYSLOG
- 802.3AH SNMP MIB

The following asymmetric configurations are not supported on the Cisco ME3600/ME3800 switches:
- efps with 1 tag & no rewrite
- efps with 2 tags & pop 1
- efps with 2 tags and no rewrite

The following asymmetric configurations are supported on the Cisco ME3600/ME3800 switches:
- efps with no tag & no rewrite
- efps with 1 tag & pop 1
- efps with 2 tag & pop 2

**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.

- Default Ethernet CFM Configuration, page 34-7
- Ethernet CFM Configuration Guidelines, page 34-8
- Configuring the CFM Domain, page 34-8
- Configuring Ethernet CFM Crosscheck, page 34-11
- Configuring Static Remote MEP, page 34-13
- Configuring a Port MEP, page 34-14
- Configuring SNMP Traps, page 34-15
- Configuring Fault Alarms, page 34-16
- Configuring IP SLAs CFM Operation, page 34-17
- Configuring CFM on EVC Bridge Domains and EVC Cross-Connect Interfaces, page 34-21

**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 service, 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 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.
- CFM is supported on VLAN interfaces and on service instances (bridge domains).
- CFM is supported on trunk ports and access 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.
- 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.
- You cannot configure tunnel mode by using the native VLAN as the S-VLAN or the C-VLAN.
- Do not configure double-tagged 802.1ag CFM packets entering a trunk port.

**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.

<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>ethernet cfm ieee</td>
</tr>
<tr>
<td></td>
<td>Configure the CFM version as IEEE 802.1ag.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ethernet cfm global</td>
</tr>
<tr>
<td></td>
<td>Globally enable Ethernet CFM on the switch.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ethernet cfm traceroute cache [size entries</td>
</tr>
<tr>
<td></td>
<td>hold-time minutes]</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For size, 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>• (Optional) For hold-time, enter the maximum cache hold time in minutes. The range is from 1 to 65535; the default is 100 minutes.</td>
</tr>
</tbody>
</table>
### Configuring Ethernet OAM, CFM, and E-LMI

#### Chapter 34

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 5     | ethernet cfm mip auto-create level level-id vlan vlan-id | (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.  
**Note** Configure MIP auto-creation only for VLANs that MIPs should monitor. Configuring for all VLANs can be CPU and memory-intensive. |
| 6     | ethernet cfm mip filter | (Optional) Enable MIP filtering, which means that all CFM frames at a lower level are dropped. The default is disabled. |
| 7     | 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. |
| 8     | id {mac-address domain_number | dns name | null} | (Optional) Assign a maintenance domain identifier.  
- **mac-address domain_number**—Enter the MAC address and a domain number. The number can be from 0 to 65535.  
- **dns name**—Enter a DNS name string. The name can be a maximum of 43 characters.  
- **null**—Assign no domain name. |
| 9     | service {ma-name | ma-number | vpn-id vpn} {evc evc-id} {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.  
- **evc evc-id**—enter an EVC name.  
- (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. |
| 10    | continuity-check | Enable sending and receiving of continuity check messages. |
| 11    | 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. |
### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 12</td>
<td>continuity-check loss-threshold threshold-value</td>
<td>(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>
<tr>
<td>Step 13</td>
<td>maximum meps value</td>
<td>(Optional) Configure the maximum number of MEPs allowed across the network. The range is from 1 to 65535. The default is 100.</td>
</tr>
<tr>
<td>Step 14</td>
<td>sender-id { chassis</td>
<td>none }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• chassis—Send the chassis ID (host name).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• none—Do not include information in the sender ID.</td>
</tr>
<tr>
<td>Step 15</td>
<td>mip auto-create { lower-mep-only</td>
<td>none }</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• lower-mep-only—Create a MIP only if there is a MEP for the service in another domain at the next lower active level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• none—No MIP auto-create.</td>
</tr>
<tr>
<td>Step 16</td>
<td>exit</td>
<td>Return to ethernet-cfm configuration mode.</td>
</tr>
<tr>
<td>Step 17</td>
<td>mip auto-create { lower-mep-only }</td>
<td>(Optional) Configure auto creation of MIPs for the domain.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• lower-mep-only—Create a MIP only if there is a MEP for the service in another domain at the next lower active level.</td>
</tr>
<tr>
<td>Step 18</td>
<td>mep archive-hold-time minutes</td>
<td>(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.</td>
</tr>
<tr>
<td>Step 19</td>
<td>exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 20</td>
<td>interface interface-id</td>
<td>Specify an interface to configure, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 21</td>
<td>switchport mode trunk</td>
<td>(Optional) Configure the port as a trunk port.</td>
</tr>
<tr>
<td>Step 22</td>
<td>ethernet cfm mip level level-id</td>
<td>(Optional) Configure a customer level or service-provider level maintenance intermediate point (MIP) for the interface. The MIP level range is 0 to 7.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
</tbody>
</table>
Chapter 34 Configuring Ethernet OAM, CFM, and E-LMI

Configuring Ethernet CFM

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
Switch(config-ecfm)# service test vlan 5
Switch(config-ecfm-srv)# continuity-check
Switch(config-ecfm-srv)# exit
Switch(config-ecfm)# exit
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ethernet cfm mep domain abc mpid 222 vlan 5
Switch(config-if-ecfm-mep)# exit
```

Configuring Ethernet CFM Crosscheck

Beginning in privileged EXEC mode, follow these steps to configure Ethernet CFM crosscheck:

```
Step 1
Command
configure terminal
Purpose
Enter global configuration mode.

Step 2
Command
ethernet cfm mep crosscheck start-delay delay
Purpose
Configure the number of seconds that the device waits for remote MEPs to come up before the crosscheck is started. The range is 1 to 65535; the default is 30 seconds.

Step 3
Command
ethernet cfm domain domain-name level level-id
Purpose
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.
```
### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>service ( \text{ma-name}</td>
<td>\text{ma-number}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- \text{ma-name}—a string of no more than 100 characters that identifies the MAID.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- \text{ma-number}—a value from 0 to 65535.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- \text{vpn-id vpn}—enter a VPN ID as the \text{ma-name}.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- \text{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></td>
<td>- \text{evc evc-id}—enter and EVC name.</td>
</tr>
<tr>
<td>5</td>
<td>mep mpid identifier</td>
<td>Define the MEP maintenance end point identifier in the domain and service. The range is 1 to 4094.</td>
</tr>
<tr>
<td>6</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>7</td>
<td>ethernet cfm mep crosscheck {enable</td>
<td>disable} domain domain-name {vlan vlan-id</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- \text{domain domain-name}—Specify the name of the created domain.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- \text{vlan} {vlan-id</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- \text{port}—Identify a port MEP.</td>
</tr>
<tr>
<td>8</td>
<td>show ethernet cfm maintenance-points remote crosscheck</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>9</td>
<td>show ethernet cfm errors [configuration]</td>
<td>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.</td>
</tr>
<tr>
<td>10</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

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><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ethernet cfm domain <em>domain-name</em> level <em>level-id</em></td>
</tr>
</tbody>
</table>
| **Step 3** | service {ma-name | ma-number | vpn-id vpn} {evc evc-id} {vlan vlan-id [direction down] | port} | Define a customer service maintenance association name or number or a VPN ID to be associated with the domain, and a VLAN ID or peer 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*—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 4** | continuity-check | Enable sending and receiving of continuity check messages. |
| **Step 5** | mep mpid *identifier* | Define the static remote maintenance end point identifier. The range is 1 to 4094. |
| **Step 6** | continuity-check static rme | Enable checking of the incoming continuity check message from a remote MEP that is configured in the MEP list. |
| **Step 7** | end | Return to privileged EXEC mode. |
| **Step 8** | show ethernet cfm maintenance-points remote static | Verify the configuration. |
| **Step 9** | 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 10** | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

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><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>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>
</tbody>
</table>
| **Step 3** | `service {ma-name | ma-number | vpn-id} port` Define a customer service maintenance association name or number or VPN ID to be associated with the domain, define a 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`—enter a VPN ID as the `ma-name`. |
| **Step 4** | `mep mpid identifier` Define the static remote maintenance end point identifier in the domain and service. The range is 1 to 4094. |
| **Step 5** | `continuity-check` Enable sending and receiving of continuity check messages. |
| **Step 6** | `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. |
| **Step 7** | `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. |
| **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. |
Chapter 34 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.

This is a sample configuration for a port MEP:

```bash
Switch(config)# ethernet cfm mep 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 gigabitethernet0/1
Switch(config-if)# ethernet cfm mep domain abc mpid 111 port
Switch(config-if)# end
```

Configuring SNMP Traps

Beginning in privileged EXEC mode, follow these steps to configure traps for Ethernet CFM:

```bash
Step 1 configure terminal
Enter global configuration mode.

Step 2 snmp-server enable traps ethernet cfm cc [mep-up] [mep-down] [config] [loop] [cross-connect]
(Optional) Enable Ethernet CFM continuity check traps.

Step 3 snmp-server enable traps ethernet cfm crosscheck [mep-unknown] [mep-missing] [service-up]
(Optional) Enable Ethernet CFM crosscheck traps.

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.
```

Use the `no` form of each command to remove a configuration or to return to the default settings.
Configuring Ethernet CFM

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><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
</tbody>
</table>
| **Step 2**  | ethernet cfm alarm notification { all | error-xcon | mac-remote-error-xcon | none | remote-error-xcon | xcon }  | Globally enable Ethernet CFM fault alarm notification for the specified defects:  
• all—report all defects.  
• error-xcon—Report only error and connection defects.  
• mac-remote-error-xcon—Report only MAC-address, remote, error, and connection defects.  
• none—Report no defects.  
• remote-error-xcon—Report only remote, error, and connection defects.  
• xcon—Report only connection defects. |
| **Step 3**  | ethernet cfm alarm delay value  | (Optional) Set a delay period before a CFM fault alarm is sent. The range is 2500 to 10000 milliseconds (ms). The default is 2500 ms. |
| **Step 4**  | ethernet cfm alarm reset value  | (Optional) Specify the time period before the CFM fault alarm is reset. The range is 2500 to 10000 milliseconds (ms). The default is 10000 ms. |
| **Step 5**  | ethernet cfm logging alarm ieee  | Configure the switch to generate system logging messages for the alarms. |
| **Step 6**  | interface interface-id  | (Optional) Specify an interface to configure, and enter interface configuration mode. |
| **Step 7**  | ethernet cfm mep domain domain-name mpid 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. The range is 1 to 4094.  
• 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. |
Chapter 34 Configuring Ethernet OAM, CFM, and E-LMI

Configuring Ethernet CFM

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.

For more information about configuring IP SLAs Ethernet operation, see the IP SLAs for Metro-Ethernet feature module at this URL:

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 34-17
- Configuring an IP SLAs Operation with Endpoint Discovery, page 34-19

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>Step 1</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>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<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>

Use the no form of each command to remove a configuration or to return to the default settings.
### Chapter 34 Configuring Ethernet OAM, CFM, and E-LMI

#### Configuring Ethernet CFM

**Step 3**

```
ethernet echo mpid identifier domain domain-name vlan vlan-id
```

or

```
ethernet jitter mpid identifier domain domain-name vlan vlan-id [interval interpacket-interval] [num-frames number-of frames transmitted]
```

Configure the IP SLAs operation as an echo (ping) or jitter operation, and enter IP SLAs Ethernet echo configuration mode.

- Enter `echo` for a ping operation or `jitter` for a jitter operation.
- For `mpid identifier`, enter a maintenance endpoint identifier. The identifier must be unique for each VLAN. The range is 1 to 4094.
- For `domain domain-name`, enter the CFM domain name.
- For `vlan vlan-id`, the VLAN range is from 1 to 4095.
- (Optional—for jitter only) Enter the `interval` between sending of jitter packets.
- (Optional—for jitter only) Enter the `num-frames` and the number of frames to be sent.

**Step 4**

```
cos cos-value
```

(Optional) Set a class of service value for the operation.

**Step 5**

```
frequency seconds
```

(Optional) Set the rate at which the IP SLAs operation repeats. The range is from 1 to 604800 seconds; the default is 60 seconds.

**Step 6**

```
history history-parameter
```

(Optional) Specify parameters for gathering statistical history information for the IP SLAs operation.

**Step 7**

```
owner owner-id
```

(Optional) Configure the SNMP owner of the IP SLAs operation.

**Step 8**

```
request-data-size bytes
```

(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.

**Step 9**

```
tag text
```

(Optional) Create a user-specified identifier for an IP SLAs operation.

**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.
Configuring Ethernet CFM

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><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>ip sla ethernet-monitor operation-number</code></td>
<td>Begin configuration of an IP SLAs automatic Ethernet operation, and enter IP SLAs Ethernet monitor configuration mode.</td>
</tr>
</tbody>
</table>
### Command

**Step 3**  
**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]

Configure the automatic Ethernet operation to create echo (ping) or jitter operation and enter IP SLAs Ethernet echo configuration mode.

- Enter **type echo** for a ping operation or **type jitter** for a jitter operation.
- For **mpid identifier**, enter a maintenance endpoint identifier. The range is 1 to 4094.
- For **domain domain-name**, enter the CFM domain name.
- For **vlan vlan-id**, the VLAN range is from 1 to 4095.
- (Optional) Enter **exclude-mpids mp-ids** to exclude the specified maintenance endpoint identifiers.
- (Optional—for jitter only) Enter the **interval** between sending of jitter packets.
- (Optional—for jitter only) Enter the **num-frames** and the number of frames to be sent.

**Step 4**  
**cos cos-value**  
(Optional) Set a class of service value for the operation.

**Step 5**  
**owner owner-id**  
(Optional) Configure the SNMP owner of the IP SLAs operation.

**Step 6**  
**request-data-size bytes**  
(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.

**Step 7**  
**tag text**  
(Optional) Create a user-specified identifier for an IP SLAs operation.

**Step 8**  
**threshold milliseconds**  
(Optional) Specify the upper threshold value in milliseconds for calculating network monitoring statistics. The range is 0 to 2147483647; the default is 5000.

**Step 9**  
**timeout milliseconds**  
(Optional) Specify the amount of time in milliseconds 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 10**  
**exit**  
Return to global configuration mode.
To remove an IP SLAs operation, enter the `no ip sla operation-number` global configuration command.

### Configuring CFM on EVC Bridge Domains and EVC Cross-Connect Interfaces

The following examples show how to configure CFM on EVC.

### Configuring CFM on EVC Commands

The following example shows the CLIs that are available for configuring CFM on EVC.

```
ethernet cfm ieee
ethernet cfm global
ethernet cfm domain L6 level 6
  service vlan100 evc evc100 direction down
  continuity-check
  service vlan200 evc evc200
  continuity-check
  service vlan200 evc evc300
  continuity-check
```
Configuring CFM on an EVC Bridge Domain

The following example shows how to configure CFM on an EVC Bridge Domain.

```
interface GigabitEthernet2/0/0
  no ip address
  no mls qos trust
  service instance 1 ethernet evc100
    encapsulation dot1q 1000
    bridge-domain 1000
    cfm mep domain L6 mpid 99
    exit
  service instance 2 ethernet evc200
    encapsulation dot1q 2000
    bridge-domain 2000
    cfm mep domain L6 mpid 77
    exit
  service instance 3 ethernet evc300
    encapsulation dot1q 300
    xconnect 1.1.1.1 1 encap mpls
    cfm mep domain L6 mpid 88
    exit
end
```

Displaying CFM on EVC

The following example shows how to display CFM information.

```
Switch# show ethernet cfm ma local
Local MEPs:
MPID Domain Name                  Lvl   MacAddress   Type  CC
Domain Id                                   Dir   Port   Id
MA Name                                           SrvcInst
EVC name
--------------------------------------------------------------------------------
77   L6                                          6     000b.45e5.cb90 BD-V  Y
     L6                                          Up    Gi 0/2   2000
     vlan2000                                          2
     evc2000
99   L6                                          6     00e0.aabb.cc00 BD-V  Y
     L6                                          Down  Gi 0/2        1000
     vlan1000                                          1
     evc1000
100  R3                                          3     00e0.aabb.cc0a BD-V  Y
     R3                                          Down  Gi 0/10        10
     sr1                                               1
     er1
2    eccm2                                       0     00e0.aabb.cc09 BD-V I
     eccm2                                       Down  Gi /0/9        100
     ser2                                          N/A
     evc2                                          N/A
--------------------------------------------------------------------------------
Total Local MEPs: 4
Local MIPs: None
```
Configuring CFM on an EVC with Cross-Connect

The following example shows how to configure CFM on EVC with cross-connect.

```plaintext
pseudowire-class vlan-xconnect
  encapsulation mpls
interface gigabit 1/1
  service instance 10 ethernet
  encapsulation dot1q 20
  xconnect 2.2.2.2 123 pw-class vlan-xconnect
  cfm mep domain Core mpid 100
```

Remote MEPs:

<table>
<thead>
<tr>
<th>MPID</th>
<th>Domain Name</th>
<th>Lvl</th>
<th>MacAddress</th>
<th>Type</th>
<th>CC</th>
</tr>
</thead>
<tbody>
<tr>
<td>7003</td>
<td>ofm_xcon</td>
<td>5</td>
<td>&lt;port-mac&gt;</td>
<td>XCONN</td>
<td>Y</td>
</tr>
<tr>
<td>8103</td>
<td>ifm_xcon</td>
<td>5</td>
<td>&lt;BRAIN-MAC&gt;</td>
<td>XCONN</td>
<td>Y</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Domain Id</th>
<th>Dir</th>
<th>Port</th>
<th>Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>ofm_xcon</td>
<td></td>
<td>Gi4/5</td>
<td>N/A</td>
</tr>
<tr>
<td>ifm_xcon</td>
<td>Up</td>
<td>(10.10.10.3,81)</td>
<td>PW</td>
</tr>
</tbody>
</table>

Managing and Displaying Ethernet CFM Information

You can use the privileged EXEC commands in these tables to clear Ethernet CFM information.

### Table 34-1 Clearing CFM Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ethernet cfm ais domain domain-name mpid id ({\text{vlan vlan-id</td>
<td>port}})</td>
</tr>
<tr>
<td>clear ethernet cfm ais link-status interface interface-id</td>
<td>Clear a SMEP out of AIS defect condition.</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 34-2 to display Ethernet CFM information.

### Table 34-2 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>domain-id]</td>
</tr>
</tbody>
</table>
Chapter 34  Configuring Ethernet OAM, CFM, and E-LMI

Managing and Displaying Ethernet CFM Information

Table 34-2  Displaying CFM Information (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<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</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
level3                                   2     3     1     100
 test                                    3     3     3     100
 name                                     4     3     1     100
 test1                                    5     2     1     100
 lck                                      6     1     1     100
Total Services : 1
```

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
-------------------------------------|----------------|-------|------|------
6307 level3                        0021.d7ee.fe80  Vlan   7    3
 vlan7                               Receive RDI      5s
```

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

<table>
<thead>
<tr>
<th>Level Port</th>
<th>MacAddress</th>
<th>SrvcInst</th>
<th>Type</th>
<th>Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>*5</td>
<td>Gi0/3</td>
<td>0021.d7ef.0700</td>
<td>N/A</td>
<td>Vlan 2,7</td>
</tr>
</tbody>
</table>

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 34-3 to display IP SLAs Ethernet CFM information.

**Table 34-3 Displaying IP SLAs CFM Information**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip sla configuration</code> [entry-number]</td>
<td>Displays configuration values including all defaults for all IP SLAs</td>
</tr>
<tr>
<td></td>
<td>operations or a specific operation.</td>
</tr>
<tr>
<td><code>show ip sla ethernet-monitor configuration</code></td>
<td>Displays the configuration of the IP SLAs automatic Ethernet operation.</td>
</tr>
<tr>
<td>[entry-number]</td>
<td></td>
</tr>
<tr>
<td><code>show ip sla statistics</code> [entry-number</td>
<td>aggregated</td>
</tr>
</tbody>
</table>

**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.
Understanding the Ethernet OAM Protocol

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.

**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 also supports 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.
Chapter 34 Configuring Ethernet OAM, CFM, and E-LMI

Setting Up and Configuring Ethernet OAM

- Default Ethernet OAM Configuration, page 34-27
- Ethernet OAM Configuration Guidelines, page 34-27
- Enabling Ethernet OAM on an Interface, page 34-27
- Enabling Ethernet OAM Remote Loopback, page 34-28
- Configuring Ethernet OAM Link Monitoring, page 34-29
- Configuring Ethernet OAM Remote Failure Indications, page 34-32
- Configuring Ethernet OAM Templates, page 34-32

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

- 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. The switch can also generate and receive Dying Gasp PDUs based on loss of power. The PDU includes a reason code to indicate why it was sent.
- 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>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Define an interface to configure as an OAM interface, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 ethernet oam</td>
<td>Enable Ethernet OAM on the interface.</td>
</tr>
</tbody>
</table>
Setting Up and Configuring Ethernet OAM

**Chapter 34      Configuring Ethernet OAM, CFM, and E-LMI**

**Step 4**

```plaintext
ethernet oam [max-rate oampdus | min-rate seconds | mode {active | passive} | timeout seconds]
```

You can configure these optional OAM parameters:

- (Optional) Enter `max-rate oampdus` to configure the maximum number of OAM PDUs sent per second. The range is from 1 to 10.
- (Optional) Enter `min-rate seconds` to configure the minimum transmission rate in seconds when one OAM PDU is sent per second. The range is from 1 to 10.
- (Optional) Enter `mode active` to set OAM client mode to active.
- (Optional) Enter `mode passive` to set OAM client mode to passive.

**Note**

When Ethernet OAM mode is enabled on two interfaces passing traffic, at least one must be in the active mode.

- (Optional) Enter `timeout seconds` to set a time for OAM client timeout. The range is from 2 to 30.

**Step 5**

```
end
```

Return to privileged EXEC mode.

**Step 6**

```
show ethernet oam status [interface interface-id]
```

Verify the configuration.

**Step 7**

```
copy running-config startup-config
```

(Optional) Save your entries in the configuration file.

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 ports that belong to an EtherChannel.

Beginning in privileged EXEC mode, follow these steps to enable Ethernet OAM remote loopback on an interface:

**Command**

**Purpose**

**Step 1**

```
configure terminal
```

Enter global configuration mode.

**Step 2**

```
interface interface-id
```

Define an interface to configure as an OAM interface, and enter interface configuration mode.
Setting Up and Configuring Ethernet OAM

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><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>interface interface-id</strong> Define an interface, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>ethernet oam link-monitor supported</strong> Enable the interface to support link monitoring. This is the default. You need to enter this command only if it has been disabled by previously entering the <strong>no ethernet oam link-monitor supported</strong> command.</td>
</tr>
</tbody>
</table>

Use the **no ethernet oam remote-loopback {supported | timeout seconds}** interface configuration command to disable remote loopback support or to remove the timeout setting.

### 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><strong>Step 3</strong></td>
<td>**ethernet oam remote-loopback {supported</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>end</strong> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>**ethernet oam remote-loopback {start</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>show ethernet oam status [interface interface-id]</strong> Verify the configuration.</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>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 4</strong> ethernet oam link-monitor symbol-period {threshold {high {high symbols</td>
<td>none}</td>
</tr>
<tr>
<td><strong>Note</strong> Repeat this step to configure both high and low thresholds.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> ethernet oam link-monitor frame {threshold {high {high-frames</td>
<td>none}</td>
</tr>
<tr>
<td><strong>Note</strong> Repeat this step to configure both high and low thresholds.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> ethernet oam link-monitor frame-period {threshold {high {high-frames</td>
<td>none}</td>
</tr>
<tr>
<td><strong>Note</strong> Repeat this step to configure both high and low thresholds.</td>
<td></td>
</tr>
</tbody>
</table>
### Setting Up and Configuring Ethernet OAM

#### Step 7

**Command:**

```
ethernet oam link-monitor frame-seCONDS
   { threshold { high { high-frames | none } | low { low-frames } } | window milliseconds }
```

**Purpose:** (Optional) Configure high and low thresholds for the frame-seCONDS error that triggers an error-frame-seCONDS link event.

- Enter `threshold high high-frames` to set a high error frame-seCONDS 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 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 polling window size in number of milliseconds. 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

**Command:**

```
[no] ethernet link-monitor on
```

**Purpose:** (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

**Command:**

```
end
```

**Purpose:** Return to privileged EXEC mode.

#### Step 11

**Command:**

```
show ethernet oam status [interface interface-id]
```

**Purpose:** Verify the configuration.

#### Step 12

**Command:**

```
copy running-config startup-config
```

**Purpose:** (Optional) Save your entries in the configuration file.

The `ethernet oam link-monitor transmit-crc { threshold { high { high-frames | none } | low { low-frames } } | window milliseconds }` 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 34 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</td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id Define an interface, and enter interface configuration mode.</td>
</tr>
</tbody>
</table>
| Step 3  | ethernet oam remote-failure {critical-event | dying-gasp | link-fault} action error-disable-interface Configure the Ethernet OAM remote-failure action on the interface. You can configure disabling the interface for one of these conditions:  
  - Select critical-event to shut down the interface when an unspecified critical event has occurred.  
  - Select dying-gasp to shut down the interface when Ethernet OAM is disabled or the interface enters the error-disabled state.  
  - Select link-fault to shut down the interface when the receiver detects a loss of signal. |
| Step 4  | end Return to privileged EXEC mode. |
| Step 5  | show ethernet oam status [interface interface-id] Verify the configuration. |
| Step 6  | copy running-config startup-config (Optional) Save your entries in the configuration file. |

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 with reason codes when Ethernet OAM is disabled, the interface is shut down, the interface enters the error-disabled state, or the switch is reloading. It can also respond to and 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>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>template template-name</code></td>
<td>Create a template, and enter template configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ethernet oam link-monitor receive-crc</code></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>{ threshold high [high-frames</td>
<td>none]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>window milliseconds]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter <code>threshold high high-frames</code> 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></td>
<td>• Enter <code>threshold high none</code> to disable the high threshold.</td>
</tr>
<tr>
<td></td>
<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></td>
<td>• Enter <code>window milliseconds</code> 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>Step 4</td>
<td><code>ethernet oam link-monitor symbol-period</code></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>{ threshold high [high-symbols</td>
<td>none]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>window symbols}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter <code>threshold high high-symbols</code> to set a high threshold in number of symbols. The range is 1 to 65535.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter <code>threshold high none</code> to disable the high threshold.</td>
</tr>
<tr>
<td></td>
<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></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>
</tbody>
</table>
### Setting Up and Configuring Ethernet OAM

**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 milliseconds` 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 34-4 to display 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 up MEPs at the UNI).
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:

- Remote UNI name and status
- Remote UNI counts

The ME 3800X and ME 3600X switch can be only a customer-edge device.

### Configuring E-LMI

Most E-LMI 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.

The switch supports only E-LMI-CE configuration.

- Default E-LMI Configuration, page 34-36
- E-LMI Configuration Guidelines, page 34-36
- Enabling E-LMI, page 34-37
- Enabling Ethernet OAM, page 34-39
- Ethernet OAM and CFM Configuration Example, page 34-39

### Default E-LMI Configuration

Ethernet LMI is globally disabled 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 UNIs defined. UNI bundling service is bundling with multiplexing.

### E-LMI Configuration Guidelines

The switch supports E-LMI only for the customer edge. The provider 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.
- You cannot configure E-LMI on VLAN interfaces.
- You must enter the `ethernet lmi ce` global configuration command to enable the switch or interface in customer-edge mode.
Enabling E-LMI

You can enable E-LMI globally or on an interface and configure the switch as 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>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 lmi global</td>
</tr>
<tr>
<td>Step 3</td>
<td>ethernet lmi ce</td>
</tr>
<tr>
<td>Step 4</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 5</td>
<td>ethernet lmi interface</td>
</tr>
<tr>
<td>Step 6</td>
<td>ethernet lmi {n391 value</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 7</td>
<td>end</td>
</tr>
<tr>
<td>Step 8</td>
<td>show ethernet lmi</td>
</tr>
<tr>
<td>Step 9</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

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.

Customer-Edge Device Configuration

This example shows the commands necessary to configure E-LMI on the CE device. The switch can only be configured as the CE device. The example enables E-LMI globally, but you can also enable it only on a specific interface.

```
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 vlan-ids` interface configuration command. Allowed VLANs can receive and send traffic on the interface in tagged format when in trunking mode.

Displaying E-LMI

You can use the privileged EXEC commands in Table 34-5 to display E-LMI information.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ethernet lmi statistics interface interface-id</code></td>
<td>Displays Ethernet LMI interface statistics sent to the CE from the status request poll.</td>
</tr>
<tr>
<td><code>show ethernet lmi uni map interface [interface-id]</code></td>
<td>Displays information about the E-LMI UNI VLAN map sent to the CE from the status request poll.</td>
</tr>
</tbody>
</table>

Ethernet CFM and Ethernet OAM Interaction

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:

- Enabling Ethernet OAM, page 34-39
- Ethernet OAM and CFM Configuration Example, page 34-39

For more information about CFM and interaction with Ethernet OAM, see the Ethernet Connectivity Fault Management feature module at this URL:


### 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>
<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 Define an interface to configure as an Ethernet OAM interface and enter interface configuration mode.</td>
</tr>
</tbody>
</table>
| **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 and Ethernet OAM between the customer edge and the provider edge switch.

Customer-edge switch 1 (CE1) configuration:
Chapter 34      Configuring Ethernet OAM, CFM, and E-LMI

Ethernet CFM and Ethernet OAM Interaction

Switch# config t
Switch(config)# interface gigabitethernet0/1
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 gigabitethernet0/5
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-srv)# exit

Provider-edge switch 2 (PE2) configuration:

Switch# config t
Switch(config)# interface gigabitethernet1/20
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-srv)# exit

Customer-edge switch 2 (CE2) configuration:

Switch# config t
Switch(config)# interface gigabitethernet0/1
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        Gi0/1         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        Gi0/1         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        Gi0/1         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
```

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 Cisco ME 3800X and ME 3600X switches. 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.
- 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.

Note
For more information about MPLS, see the “Multiprotocol Label Switching” section of the Cisco IOS Switching Services 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 36-2
- Understanding MPLS VPNs, page 36-3
- Configuring MPLS VPNs, page 36-6
- Understanding MPLS Traffic Engineering and Fast Reroute, page 36-17
- Configuring MPLS Traffic Engineering and Fast Reroute, page 36-19
- Understanding EoMPLS, page 36-26
- Enabling EoMPLS, page 36-30
- Support for H-VPLS, page 36-45
- Understanding MPLS OAM, page 36-57
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.

The ME 3800X and ME 3600X switches perform these LSR operations:

- Swap and forward
  The switch removes the top label, adds from 1 to 4 labels, then forwards the packet to the specified adjacency with no Layer 2 or Layer 3 lookup.
Chapter 36 Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS

Understanding MPLS VPNs

Pop and forward
The switch removes the top label in the packet and forwards the packet to the specified adjacency.

Pop and lookup
The switch removes the top label and performs a lookup based on the exposed packet.
The type of lookup is determined by the popped label. The lookup could be:
- IPv4—the label specifies a VRF or global table to be used for an IPv4 lookup.
- MPLS Label—The switch performs a lookup on the exposed label. The exposed label might specify a Swap or Pop operation. The switch performs up to three recursive MPLS label lookups in the ternary content addressable memory (TCAM).

Drop packet
The switch drops the packet based on lookup of the top label.

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.

The ME 3800X and ME 3600X switches support Label Distribution Protocol (LDP) session protection to maintain an LDP session during a link failure. LDP session protection eliminates the need for the link neighbor to relearn the prefix label bindings when the link recovers.

Provider Edge Routers (PE) operate at the edge of the provider network. They perform Label Edge Router (LER) imposition and disposition operations at the edge of an MPLS network. In an MPLS network, the ingress edge router receives the packet and adds a label to the packet. The egress edge router removes the label.

The ME 3800X and ME 3600X switches perform these operations:
- Push
  The ingress switch adds one or more labels.
- Pop
  The egress switch removes a label and forwards the packet.

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 36-1 shows an example of a VPN with a service-provider backbone network, provider-edge (PE) and customer leading-edge (CLE) routers and customer-edge (CE) devices.

**Figure 36-1  VPNs with a Service-Provider Backbone**

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 36-2 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
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, or through a routing protocol, such as OSPF, EIGRP and Routing Information Protocol (RIP), with the CE device. 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 EBGP). 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 switch used as a PE router:

- Default MPLS Configuration, page 36-7
- MPLS VPN Configuration Guidelines, page 36-7
These sections describe the required tasks:

- Enabling MPLS, page 36-7
- Defining VPNs, page 36-8
- Configuring BGP Routing Sessions, page 36-9
- Configuring Provider-Edge-to-Provider-Edge Routing Sessions, page 36-10

You must also configure a provider-edge-to-customer-edge routing session. These sections provide example configurations:

- Configuring Provider-Edge-to-Customer-Edge Routing Sessions, page 36-11
- BGP Provider-Edge-to-Customer-Edge Configuration, page 36-11
- OSPF Provider-Edge-to-Customer-Edge Configuration, page 36-12
- RIPv2 Provider-Edge-to-Customer-Edge Routing Sessions, page 36-13
- Configuring Static Route Provider-Edge-to-Customer-Edge Routing Sessions, page 36-14
- EIGRP Provider-Edge-to-Customer-Edge Configuration, page 36-14

For an example of packet flow in an MPLS VPN, see the “Packet Flow in an MPLS VPN” section on page 36-15.

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 label protocol is explicitly configured for an interface, the default label distribution protocol for the switch is used by the Label Distribution Protocol (LDP). 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 29-95.
- The switch supports MPLS forwarding on the following interfaces:
  - Routed ports
  - Routed EtherChannels

Note

Some MPLS features require specific software licenses.

Enabling MPLS

To use MPLS in a network, such as the one shown in Figure 36-1, 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>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 on the switch if it is disabled.</td>
</tr>
<tr>
<td>Step 3 mpls label protocol ldp</td>
<td>Set the label protocol on the switch to LDP. The default protocol is TDP.</td>
</tr>
<tr>
<td>Step 4 interface Loopback0</td>
<td>Enter interface configuration mode for a loopback interface.</td>
</tr>
<tr>
<td>Step 5 ip address ip address</td>
<td>Assign an IP address to the loopback interface.</td>
</tr>
<tr>
<td></td>
<td>The subnet mask value has to be a host mask, /32.</td>
</tr>
<tr>
<td>Step 6 mpls ldp router-id loopback 0 force</td>
<td>Specify the interface to force the loopback.</td>
</tr>
<tr>
<td>Step 7 interface interface-id</td>
<td>Enter interface configuration mode, and specify the Layer 3 interface connected to the MPLS network. Valid interfaces include 10GigabitEthernet1/1/1, GigabitEthernet1/1/2, and VLANs.</td>
</tr>
<tr>
<td>Step 8 ip address ip address</td>
<td>Assign an IP address to the Layer 3 interface connected to the MPLS network.</td>
</tr>
<tr>
<td>Step 9 mpls ip</td>
<td>Enable MPLS forwarding of IPv4 packets along normally routed paths for the interface.</td>
</tr>
<tr>
<td>Step 10 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 11 show mpls forwarding-table</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>Step 12 show mpls interfaces</td>
<td></td>
</tr>
<tr>
<td>Step 13 show mpls ldp neighbor</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>Step 14 show mpls ldp discovery</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>Step 15 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</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 disable LDP.

### Defining VPNs

**Note** Before defining VPNs, enable MPLS on the switch (see *Enabling MPLS*, page 36-7).
Beginning in privileged EXEC mode, follow these steps to define VPN routing instances on the PE router:

<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 routing is disabled).</td>
</tr>
<tr>
<td>3</td>
<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>4</td>
<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>
<tr>
<td>5</td>
<td>route-target [export</td>
<td>import</td>
</tr>
<tr>
<td>6</td>
<td>import map route-map</td>
<td>(Optional) Associate the specified import route map with the VRF.</td>
</tr>
<tr>
<td>7</td>
<td>export map route-map</td>
<td>(Optional) Associate the specified export route map with the VRF.</td>
</tr>
<tr>
<td>8</td>
<td>exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>9</td>
<td>interface interface-id</td>
<td>Enter interface configuration mode, and specify the Layer 3 ES or VLAN interface to be associated with the VRF.</td>
</tr>
<tr>
<td>10</td>
<td>ip vrf forwarding vrf-name</td>
<td>Associate the Layer 3 interface with the VRF.</td>
</tr>
<tr>
<td>11</td>
<td>ip address ip address</td>
<td>Add the VRF route to the VRF routing table.</td>
</tr>
<tr>
<td>12</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>13</td>
<td>show ip vrf</td>
<td>Display the defined VRFs and interfaces.</td>
</tr>
<tr>
<td>14</td>
<td>show ip route vrf</td>
<td>Display the IP routing table for a VRF.</td>
</tr>
<tr>
<td></td>
<td>show ip cef vrf vrf-name</td>
<td>Display the CEF forwarding table associated with a VRF.</td>
</tr>
<tr>
<td>15</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 vrf vrf-name global configuration command to delete a VRF and remove interfaces from it. Use the no ip vrf forwarding interface configuration command to remove an interface from a VRF.

## 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>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 routing is disabled).</td>
</tr>
</tbody>
</table>
### Configuring MPLS VPNs

Use the `no router bgp autonomous-system` global configuration command to delete the BGP routing session.

#### Configuring Provider-Edge-to-Provider-Edge Routing Sessions

You can configure provider-edge-to-provider-edge (PE-PE) routing sessions using IBGP or BGP.

#### IBGP Provider-Edge-to-Provider-Edge Configuration

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><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>router bgp autonomous-system-number</code></td>
<td>Enter router configuration mode.</td>
</tr>
<tr>
<td><code>address-family vpv4 [unicast]</code></td>
<td>Enter address family configuration mode to configure routing sessions that use standard VPNv4 address prefixes. (Optional) <code>unicast</code>—Specify VPNv4 unicast address prefixes.</td>
</tr>
<tr>
<td><code>neighbor ip-address activate</code></td>
<td>Activate the advertisement of the IPv4 address family.</td>
</tr>
<tr>
<td><code>neighbor ip address send-community extended</code></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>show ip bgp</code></td>
<td>Verify BGP configuration. Display information about all BGP IPv4 prefixes.</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>

Use the `no router bgp autonomous-system` global configuration command to delete the BGP routing session.
IBGP Provider-Edge-to-Provider-Edge Configuration

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 Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>router bgp autonomous-system-number Enter router configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>address-family ipv4 Enter address family configuration mode to configure a routing session using IPv4.</td>
</tr>
<tr>
<td>Step 4</td>
<td>neighbor ip-address activate Activate the advertisement of the IPv4 address family.</td>
</tr>
<tr>
<td>Step 5</td>
<td>end Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>show ip bgp [ipv4] [neighbors] [vpnv4] Verify BGP configuration. Display information about all BGP IPv4 prefixes.</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>

Use the no router bgp autonomous-system global configuration command to delete the BGP routing session.

Configuring Provider-Edge-to-Customer-Edge Routing Sessions

You can configure provider-edge-to-customer-edge (PE-CE) routing sessions using any of these protocols:

- BGP
- OSPF
- RIPv2
- Static Route
- EIGRP

BGP Provider-Edge-to-Customer-Edge Configuration

Beginning in privileged EXEC mode, follow these steps on the provider-edge router to configure a provider-edge-to-customer-edge (PE-to-CE) routing session in a provider network that uses BGP:

<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 bgp autonomous-system-number 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 Define EGP routing parameters for PE-to-CE routing sessions, and enter VRF address-family configuration mode.</td>
</tr>
</tbody>
</table>

Note The default is off for auto-summary and synchronization in the VRF address-family configuration mode.
### OSPF Provider-Edge-to-Customer-Edge Configuration

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 OSPF:

<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 ospf process-id vrf vrf-name</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>network ip-address area area-id</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>router-id ip-address</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>domain-id ip-address</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>router ospf process-id vrf vrf-name</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>redistribute bgp as-number subnets [metric metric-value] [metric-type {1</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>router bgp as-number address-family ipv4 [unicast] vrf vrf-name redistribute ospf process-id [match {internal</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>show ip bgp vpnv4 vrf vrf-name</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>show ip route vrf vrf-name</td>
</tr>
</tbody>
</table>

Use the `no router bgp as-number` global configuration command to delete the BGP routing session.
### RIPv2 Provider-Edge-to-Customer-Edge Routing Sessions

Beginning in privileged EXEC mode, follow these steps on the provider-edge router to configure RIPv2 PE-to-CE routing:

<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 rip</td>
<td>Enable RIP routing, and enter router configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>version 2</td>
<td>Configure RIPv2.</td>
</tr>
<tr>
<td>4</td>
<td>address-family ipv4 [unicast] vrf vrf-name</td>
<td>Define RIP 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>5</td>
<td>network ip-address</td>
<td>Enable RIP on the PE-to-CE link.</td>
</tr>
<tr>
<td>6</td>
<td>router bgp as-number</td>
<td>Redistribute per-VRF RIP routes in MBGP.</td>
</tr>
<tr>
<td></td>
<td>address-family ipv4 [unicast] vrf vrf-name redistribute rip</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>router rip</td>
<td>Enable RIP routing, and enter router configuration mode.</td>
</tr>
<tr>
<td>8</td>
<td>version 2</td>
<td>Configure RIPv2.</td>
</tr>
<tr>
<td>9</td>
<td>address-family ipv4 [unicast] vrf vrf-name</td>
<td>Define RIP 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>10</td>
<td>redistribute bgp as-number [metric] [transparent]</td>
<td>Redistribute MP-IBGP VPNv4 prefixes in RIP.</td>
</tr>
<tr>
<td>11</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>12</td>
<td>show ip rip database [network-prefix]</td>
<td>Display summary address entries in the RIP routing database entries.</td>
</tr>
<tr>
<td>13</td>
<td>show ip bgp vpnv4 vrf vrf-name</td>
<td>Display VPNv4 address information from the BGP table.</td>
</tr>
<tr>
<td>14</td>
<td>show ip route vrf vrf-name</td>
<td>Display the IP routing table associated with a VRF instance.</td>
</tr>
<tr>
<td>15</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 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</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip route vrf vrf-name prefix mask [next-hop-address] [interface interface-number] [global] [distance] [permanent] [tag tag]</td>
</tr>
<tr>
<td>Step 3</td>
<td>router bgp as-number address-family ipv4 [unicast] vrf vrf-name</td>
</tr>
<tr>
<td>Step 4</td>
<td>redistribute connected or network network-number [mask network-mask] [route-map map-name]</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Step 6</td>
<td>show ip bgp vpnv4 vrf vrf-name</td>
</tr>
<tr>
<td>Step 7</td>
<td>show ip route vrf vrf-name</td>
</tr>
<tr>
<td>Step 8</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

**EIGRP Provider-Edge-to-Customer-Edge Configuration**

Beginning in privileged EXEC mode, follow these steps on the provider-edge router to configure a provider-edge-to-customer-edge (PE-to-CE) routing session in a provider network that uses EIGRP:

<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 autonomous-system-number</td>
</tr>
<tr>
<td>Step 3</td>
<td>address-family ipv4 [unicast] vrf vrf-name</td>
</tr>
</tbody>
</table>
| Step 4  | network ip-address wildcard-mask | Specify the network for the VRF.  
• The network statement is used to identify which interfaces to include in EIGRP. The VRF must be configured with addresses that fall within the wildcard-mask range of the network statement. |
Use the `no router eigrp as-number` global configuration command to delete the EIGRP routing session.

### Packet Flow in an MPLS VPN

Figure 36-3 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 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.

### Sample Configurations

This example shows a Layer 3 VPN configured on an EFP:

```bash
Switch# show run interface g0/24
Building configuration...

Current configuration : 226 bytes
!
interface GigabitEthernet0/24
  port-type nni
  switchport trunk allowed vlan none
  switchport mode trunk
  service instance 1 ethernet
  encapsulation dot1q 20
  rewrite ingress tag pop 1 symmetric
  bridge-domain 100
!
end
```

This example shows a Layer 3 VPN configured using non-switchport port mode:

```bash
Switch# show run interface g0/24
interface GigabitEthernet0/24
  port-type nni
  no switchport
  ip vrf forwarding A
  ip address 100.1.1.1 255.255.255.0
```

This example shows a Layer 3 VPN configured on a switchport:

```bash
Switch# show run interface g0/24
interface GigabitEthernet0/24
  port-type nni
  switchport access vlan 100
```
Understanding MPLS Traffic Engineering and Fast Reroute

This section describes the switch support of MPLS traffic engineering (TE) and includes these sections:

- MPLS TE, page 36-17
- MPLS TE Fast Reroute, page 36-18
- MPLS TE Primary and Backup Autotunnel, page 36-19

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 number of supported tunnels depends upon the installed license. Refer to the licensing document.

The 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 \texttt{ip explicit-path} global configuration mode to enter explicit-path configuration mode and then use the \texttt{exclude-address} command to specify addresses to exclude from the path.

For information about load balancing, see this URL:
• 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.

• Prefix-independent fast reroute.

The 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.

---

**Note**

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 `ip rsvp signalling hello [fast reroute] refresh` global configuration command.

**Note**
The `ip rsvp signalling hello [fast reroute] refresh` command is needed only when loss of signal cannot be detected.

Backup tunnels have these characteristics on the 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 MPLS TE on a switch:

- Default MPLS TE and Fast Reroute Configuration, page 36-19
- MPLS TE and Fast Reroute Configuration Guidelines, page 36-20

These sections describe the configuration procedures:

- Configuring MPLS TE, page 36-20
- Configuring TE Fast Reroute, page 36-22
- Configuring Primary and Backup Autotunnels, page 36-25

**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 “Multiprotocol Label Switching (MPLS) Commands” section on page C-6 of Appendix C, “Unsupported Commands in Cisco IOS Release 15.1(2)EY.”
- 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:

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>mpls traffic-eng tunnels</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip rsvp signalling hello</td>
</tr>
<tr>
<td>Step 4</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 5</td>
<td>mpls traffic-eng tunnels</td>
</tr>
<tr>
<td>Step 6</td>
<td>ip rsvp bandwidth bandwidth</td>
</tr>
<tr>
<td>Step 7</td>
<td>ip rsvp signalling hello</td>
</tr>
<tr>
<td>Step 8</td>
<td>end</td>
</tr>
<tr>
<td>Step 9</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>
<tr>
<td>Step 6</td>
<td>tunnel mpls traffic-eng aut routed announce</td>
</tr>
<tr>
<td>Step 7</td>
<td>tunnel mpls traffic-eng priority</td>
</tr>
<tr>
<td>Step 8</td>
<td>tunnel mpls traffic-eng bandwidth bandwidth</td>
</tr>
<tr>
<td>Step 9</td>
<td>tunnel mpls traffic-eng fast-reroute</td>
</tr>
<tr>
<td>Step 10</td>
<td>tunnel mpls traffic-eng path-option 1 explicit name name</td>
</tr>
<tr>
<td>Step 11</td>
<td>tunnel mpls traffic-eng path-option 2 dynamic</td>
</tr>
<tr>
<td>Step 12</td>
<td>exit</td>
</tr>
<tr>
<td>Step 13</td>
<td>ip explicit-path name name</td>
</tr>
<tr>
<td>Step 14</td>
<td>next-address A.B.C.E</td>
</tr>
<tr>
<td>Step 15</td>
<td>next-address A.B.C.F</td>
</tr>
<tr>
<td>Step 16</td>
<td>exclude-address A.B.C.X</td>
</tr>
<tr>
<td>Step 17</td>
<td>end</td>
</tr>
<tr>
<td>Step 18</td>
<td>show ip explicit-paths</td>
</tr>
<tr>
<td>Step 19</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

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:

<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 {isis</td>
<td>ospf}</td>
</tr>
<tr>
<td>Step 3 mpls traffic-eng {level-1</td>
<td>level-2}</td>
</tr>
<tr>
<td>or mpls traffic-eng area 0</td>
<td>Turn on MPLS traffic engineering for OSPF.</td>
</tr>
<tr>
<td>Step 4 mpls traffic-eng router-id loopback0</td>
<td>Specify the traffic engineering router identifier for the node to be the IP address associated with interface loopback0.</td>
</tr>
<tr>
<td>Step 5 metric-style wide</td>
<td>Configure a router to generate and accept only new-style stands for type, length, and value objects (TLVs).</td>
</tr>
<tr>
<td>Note</td>
<td>This command is for IS-IS routing only.</td>
</tr>
<tr>
<td>Step 6 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 7 show mpls traffic-eng</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 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>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface tunnel</td>
<td>Create a tunnel interface, and enter interface configuration mode for the tunnel interface.</td>
</tr>
<tr>
<td>tunnel-number</td>
<td></td>
</tr>
<tr>
<td>Step 3 ip unnumbered</td>
<td>Configure the tunnel source address. This is usually the IP address of the loopback0 interface. The command is not effective until loopback0 is configured with an IP address.</td>
</tr>
<tr>
<td>interface-id</td>
<td></td>
</tr>
<tr>
<td>Step 4 tunnel destination</td>
<td>Specify the IP address of the device where the tunnel terminates. This should be the router ID of the next-hop or next-next hop of the LSP to be protected.</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 36 Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS

Configuring MPLS Traffic Engineering and Fast Reroute

Enter the `no tunnel mode mpls traffic-eng` global configuration command to disable MPLS traffic engineering.

```
no tunnel mode mpls traffic-eng
```

Configure a path option for an MPLS TE tunnel. Keywords have these meanings:

- `number`—When multiple paths are configured, lower-numbered options are preferred.
- `dynamic`—Specify that the LSP path is dynamically calculated.
- `explicit`—Specify that the LSP path is an explicit IP path.
- `name path-name`—Path name of the IP explicit path that the tunnel uses with this option.
- `name path-number`—Path number of the IP explicit path that the tunnel uses with this option.
- `(Optional) lockdown`—Specify that the LSP cannot be reoptimized.

```
tunnel mpls traffic-eng path-option number {dynamic | explicit {name path-name | path-number}} [lockdown]
```

Specify the path of the tunnel, and enter IP explicit path command mode to set up or modify the explicit path. An IP explicit path is a list of IP addresses, each representing a node or link in the explicit path.

```
ip explicit-path name path-name
```

Specify the next IP address in the explicit path.

```
ext-address A.B.C.E
```

Repeat Step 8 for additional IP addresses in the path.

```
end
```

Return to privileged EXEC mode.

```
show ip explicit-paths
```

Verify the configuration.

```
copy running-config startup-config
```

(Optional) Save your entries in the configuration file.

Enter the `no tunnel mode mpls traffic-eng global` configuration command to disable MPLS traffic engineering or the `no ip explicit-path global` 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:

```
configure terminal
```

Enter global configuration mode.

```
interface interface-id
```

Specify the interface ID of the protected link and enter interface configuration mode.

```
mls traffic-eng backup-path tunnel tunnel-id
```

Configure the interface to use a backup tunnel in the event of a detected failure on that interface. You can enter this command multiple times to associate the protected interface with multiple backup tunnels.

```
end
```

Return to privileged EXEC mode.
To remove the backup tunnel configuration, enter the `no mpls traffic-eng backup-path tunnel` interface configuration command.

### Configuring Fast Reroute Failure Detection (Optional)

This configuration is needed only when loss of signal cannot be detected.

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 Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip rsvp signalling hello Globally enable Hello signalling on the switch.</td>
</tr>
<tr>
<td>Step 3</td>
<td>interface interface-id Specify an interface ID, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip rsvp signalling hello fast-reroute refresh misses number Configure the number of consecutive RSVP TE hello acknowledgments a node can miss before the node communication with its neighbor status is down. Valid values are from 4 to 10. The default is 4.</td>
</tr>
<tr>
<td>Step 5</td>
<td>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). <strong>Note</strong> To prevent false detection of a down neighbor and unnecessarily triggering fast reroute, we recommend configuring a minimum frequency of 200 ms.</td>
</tr>
<tr>
<td>Step 6</td>
<td>ip rsvp signalling hello Enable Hello signalling on the interface.</td>
</tr>
<tr>
<td>Step 7</td>
<td>end Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 8</td>
<td>show ip rsvp fast-reroute Verify the configuration.</td>
</tr>
<tr>
<td></td>
<td>show ip rsvp hello instance summary</td>
</tr>
<tr>
<td>Step 9</td>
<td>copy running-config startup-config (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Enter the `no ip rsvp signalling hello` global configuration command to disable Hello signalling on the switch. Enter the `no ip rsvp signalling hello fast-reroute refresh misses` or the `no ip rsvp signalling hello fast-reroute refresh interval` interface configuration command to set the misses or refresh interval to the default.
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>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>mpls traffic-eng auto-tunnel primary onehop</td>
<td>Configure the switch to automatically create primary MPLS tunnels to all next hops.</td>
</tr>
<tr>
<td>3</td>
<td>mpls traffic-eng auto-tunnel primary tunnel-num [min num] [max num]</td>
<td>Configure the range of tunnel interface numbers for primary autotunnels.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) [min num]—Specify the minimum number of the primary tunnels. Valid values are from 0 to 65535. The default is 65436.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) [max num]—Specify the maximum number of the primary tunnels. The max number is the minimum number plus 99. Valid values are from 0 to 65535.</td>
</tr>
<tr>
<td>4</td>
<td>mpls traffic-eng auto-tunnel primary timers removal rerouted sec</td>
<td>Configure how many seconds after a failure primary autotunnels are removed. Valid values are 30 to 604800. The default is 0.</td>
</tr>
<tr>
<td>5</td>
<td>mpls traffic-eng auto-tunnel primary config unnumbered interface-id</td>
<td>Enable IP processing on the specified interface without an explicit address.</td>
</tr>
<tr>
<td>6</td>
<td>mpls traffic-eng auto-tunnel primary config mpls ip</td>
<td>Enable Label Distribution Protocol (LDP) on primary autotunnels.</td>
</tr>
<tr>
<td>7</td>
<td>clear mpls traffic-eng auto-tunnel primary</td>
<td>Remove all primary autotunnels and re-create them.</td>
</tr>
<tr>
<td>8</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>9</td>
<td>show interface tunnel tunnel-num</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>10</td>
<td>copy running-config startup-config</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 auto tunnels, 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:

<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>mpls traffic-eng auto-tunnel backup</td>
<td>Configure the switch to automatically create next-hop (NHOP) and next-next hop (NNHOP) backup tunnels.</td>
</tr>
<tr>
<td>3</td>
<td>mpls traffic-eng auto-tunnel backup nhop-only</td>
<td>Configure the switch to automatically build only next-hop (NHOP) backup tunnels.</td>
</tr>
</tbody>
</table>
Enter the no form of each command to delete the tunnel or disable the feature or capability.

### Understanding EoMPLS

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 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 switch supports auto-sense signaling to allow two remote PEs to negotiate VC type signaling.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>mpls traffic-eng auto-tunnel backup tunnel-num [min num] [max num]</td>
</tr>
<tr>
<td>Step 5</td>
<td>mpls traffic-eng auto-tunnel backup timers removal unused sec</td>
</tr>
<tr>
<td>Step 6</td>
<td>mpls traffic-eng auto-tunnel backup config unnumbered interface interface-id</td>
</tr>
<tr>
<td>Step 7</td>
<td>mpls traffic-eng auto-tunnel primary config mpls ip</td>
</tr>
<tr>
<td>Step 8</td>
<td>end</td>
</tr>
<tr>
<td>Step 9</td>
<td>show interface tunnel tunnel-num</td>
</tr>
<tr>
<td>Step 10</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>
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 36-27
- EoMPLS Limitations, page 36-30

### Interaction with Other Features

This section describes how EoMPLS interacts other features. It includes these sections:

- EoMPLS and IEEE 802.1Q Tunneling, page 36-27
- EoMPLS and Layer 2 Tunneling, page 36-28
- EoMPLS and Q in Q, page 36-29
- EoMPLS and QoS, page 36-30

#### 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 12, “Configuring Ethernet Virtual Connections (EVCs).”

Figure 36-4 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).
Understanding EoMPLS

By entering 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.

### 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 12, “Configuring Ethernet Virtual Connections (EVCs).”

This example shows how to configure Layer 2 tunneling:

```plaintext
Switch(config)# interface Vlan102
Switch(config-if)# no ip address
Switch(config-if)# xconnect 12.12.12.12 102 encapsulation mpls

Switch(config)# interface GigabitEthernet0/24
Switch(config-if)# switchport trunk allowed vlan none
Switch(config-if)# switchport mode trunk
Switch(config-if)# no keepalive
Switch(config-if)# service instance 1 ethernet
Switch(config-if)# encapsulation untagged
Switch(config-if)# l2protocol tunnel cdp
Switch(config-if)# bridge-domain 102
```
EoMPLS and Q in Q

When the remote PE supports Q in Q, but not VC type 4, you can use the **platform rewrite imposition tag push 1 symmetric** interface configuration command to push an additional VLAN tag to make the type 5 PW work like a Q in Q Layer 2 port.

**Note**
The command has no effect on a VC type 4 PW.

This example sends packets with VLAN 11 to EFP 1. When the packets reach the remote PE, the payload Layer 2 packets have two VLAN tags, VLAN 101 and VLAN 11.

```
Switch (config)# interface gigabitEthernet 0/15
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan none
Switch (config-if)# service instance 1 ethernet
Switch (config-if-srv)# encapsulation dot1q 11
Switch (config-if-srv)# bridge-domain 101
Switch (config-if-srv)# exit
Switch (config-if)# exit

Switch (config)# interface Vlan101
Switch (config-if)# platform rewrite imposition tag push 1 symmetric
Switch (config-if)# xconnect 12.12.12.12 300 encapsulation mpls

Switch # show running-config interface gigabitEthernet 0/15
Building configuration...

Current configuration : 188 bytes
! interface GigabitEthernet0/15
  port-type nni
  switchport trunk allowed vlan none
  switchport mode trunk
  service instance 1 ethernet
    encapsulation dot1q 11
    bridge-domain 101
! end
Switch # show running-config interface vlan 101
Building configuration...

Current configuration : 136 bytes
! interface Vlan101
  no ip address
  platform rewrite imposition tag push 1 symmetric
  xconnect 12.12.12.12 300 encapsulation mpls
end

Packets sent from the remote PE have an outer VLAN with any VLAN number and VLAN 11. The outer VLAN number is popped at this PE, and the packets are sent out from EFP 1 with VLAN 11.
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) and Layer 2 parameters (CoS). See Chapter 27, “Configuring Quality of Service (QoS)” for more information about EoMPLS and QoS.

EoMPLS Limitations

These restrictions apply to EoMPLS:

- You cannot configure MPLS and EoMPLS on the same port.
- 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.
- 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 xconnect interface configuration command. Use the xconnect command to configure pseudowire redundancy.
- IGMP—Disable IGMP for any bridge domain where pseudowire is configured.

Enabling EoMPLS

This section includes this information about configuring EoMPLS on a switch used as a provider-edge router:

- Default EoMPLS Configuration, page 36-31
- EoMPLS Configuration Guidelines, page 36-31
- Configuring EoMPLS, page 36-31
- Configuring the Pseudowire Using Pseudowire Class, page 36-33
- Configuring L2VPN Interworking, page 36-34
- EoMPLS and EVC, page 36-35
- Packet Flow in an EoMPLS Network, page 36-38
- Configuring L2VPN Pseudowire Redundancy, page 36-40
- Routed VPLS/EoMPLS, page 36-43
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:
- 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.
- You can set the maximum transmission unit (MTU) value on an SVI.

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. You use the same commands to enable port-based EoMPLS.

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>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>mpls label protocol ldp</code></td>
<td>Enable LDP for all interfaces. By default, TDP is enabled. This command causes all interfaces to use LDP.</td>
</tr>
</tbody>
</table>
Enabling EoMPLS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> interface loopback0</td>
<td>Enter interface configuration mode for a loopback interface.</td>
</tr>
<tr>
<td><strong>Step 4</strong> ip address ip-address subnet mask</td>
<td>Assign an IP address to the loopback interface.</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 vlan vlan-id or interface interface-id</td>
<td>Enter a VLAN ID (for VLAN-based EoMPLS) to enter SVI configuration mode. or Enter the interface ID of a routed port (for port-based EoMPLS), to enter routed port interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong> xconnect destination vc-id encapsulation mpls</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 8</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 9</strong> show mpls l2transport vc</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td><strong>Step 10</strong> copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the 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 routed port and PE2’s VLAN 4 interface.

PE1 has an IP address 10.0.0.1/32, and PE2 has IP address 20.0.0.1/32. 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:

```
Switch(config)# interface loopback0
Switch(config-if)# ip address 10.10.10.10 255.255.255.255
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet0/1
Switch(config-if)# xconnect 20.20.20.20 123 encapsulation mpls
```

Enter these commands on the PE2 switch:

```
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)# xconnect 10.10.10.10 123 encapsulation mpls
```

This example shows how to set the MTU value on an SVI.

```
Switch(config)# interface vlan 100
Switch(config-if)# xconnect 2.2.2.2 2 encapsulation mpls
Switch(config-if)# mtu 9000
```
Enabling EoMPLS

Configuring the Pseudowire Using Pseudowire Class

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 1</th>
<th>configure terminal</th>
<th>Enter global configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>pseudowire-class name</td>
<td>Create a pseudowire class with the specified name and enter pseudowire class configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>encapsulation mpls</td>
<td>Specify tunneling encapsulation. For AToM, the encapsulation type is <code>mpls</code>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>preferred-path interface tunnel tunnel-id</td>
<td>(Optional) Specify the path that pseudowire traffic uses to be an MPLS TE tunnel.</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 mpls l2transport vc [detail]</td>
<td>Verify the configuration.</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>

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
Local intf Local circuit Dest address VC ID Status
------------- -------------------------- --------------- ---------- ----------
Vl20 Eth VLAN 20 10.1.1.2 20 UP
Vl20 Eth VLAN 20 10.1.1.4 20 DOWN

This example shows how to display the preferred path using the `show mpls l2transport vc 2 detail` command.

Switch# show mpls l2transport vc 2 detail
Local interface: Gi0/24 up, line protocol up, Ethernet up
Destination address: 2.2.2.2, VC ID: 2, VC status: down
Output interface: none, imposed label stack {}
   Preferred path: Tunnel100, no route
   Default path:
   No adjacency
Create time: 00:00:12, last status change time: 00:00:12
Signaling protocol: LDP, peer unknown
Targeted Hello: 51.51.51.51(LDP Id) -> 2.2.2.2
Status TLV support (local/remote) : enabled/unknown (no remote binding)
   Label/status state machine : local standby, AC-ready, LnuRnd
   Last local dataplane status rcvd: no fault
   Last local SSS circuit status rcvd: no fault
   Last local SSS circuit status sent: not sent
   Last local LDP TLV status sent: not sent
   Last remote LDP TLV status rcvd: unknown (no remote binding)
MPLS VC labels: local 19, remote unassigned
Group ID: local 0, remote unknown
MTU: local 1500, remote unknown
Remote interface description:
Enabling EoMPLS

Sequencing: receive disabled, send disabled
VC statistics:
  packet totals: receive 0, send 0
  byte totals: receive 0, send 0
  packet drops: receive 0, send 0

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 switch does not support ATM interfaces, Point-to-Point Protocol (PPP), or frame relay as mentioned in this document.

L2VPN interworking on the ME 3800X and ME 3600X switches works in either Ethernet mode (VC type 5) or VLAN mode (VC type 4). 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>pseudowire-class name</td>
<td>Create a pseudowire class with the specified name and enter pseudowire class configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>encapsulation mpls</td>
<td>Specify tunneling encapsulation. For AToM, the encapsulation type is <code>mpls</code>.</td>
</tr>
<tr>
<td>4</td>
<td>interworking {ethernet</td>
<td>vlan}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <code>ethernet</code>—Send Ethernet packets across the pseudowire.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <code>vlan</code>—Send VLAN-tagged packets across the pseudowire.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Although visible in the CLI, the <code>ip</code> keyword is not supported.</td>
</tr>
<tr>
<td>5</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>6</td>
<td>show mpls l2transport vc [detail]</td>
<td>Verify the configuration.</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>
This example shows how to configure VLAN interworking:

Switch# config t
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.

### EoMPLS and EVC

When a pseudowire is configured on a VLAN interface, the pseudowire becomes a virtual Layer 2 port in that VLAN or bridge domain. You can configure other types of L2 ports, such as EFP ports and switch ports in the same bridge domain. Switch functions, such as MAC address learning, flooding, and forwarding to learned MAC addresses apply to all the Layer 2 ports, including the pseudowire.

**Note**

When EFP and a pseudowire are configured in the same bridge domain, EFP cannot be configured with the `rewrite ingress tag pop 2 symmetric` command. Other restrictions on switching between EFPs or between EFPs and switch ports also apply.

This example shows how to configure a pseudowire on a VLAN interface:

Switch(config)# interface GigabitEthernet0/1
Switch(config-if) switchport access vlan 100

Switch(config)# interface GigabitEthernet0/2
Switch(config-if) switchport mode trunk

Switch(config)# interface GigabitEthernet0/3
Switch(config-if) description all egress efps
Switch(config-if) switchport trunk allowed vlan none
Switch(config-if) switchport mode trunk
Switch(config-if) service instance 1 ethernet
Switch(config-if) encapsulation dot1q 12
Switch(config-if) bridge-domain 100

Switch(config)# interface Vlan100
Switch(config-if) no ip address
Switch(config-if) xconnect 12.12.12.12 123 encapsulation mpls

To see the MAC addresses learned from a pseudowire, enter the `show mac address-table dynamic` command. The example below shows output from the command.

Switch# show mac address-table dynamic

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Mac Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>0000.0000.0011</td>
<td>DYNAMIC</td>
<td>------</td>
</tr>
<tr>
<td>100</td>
<td>0000.0000.00bb</td>
<td>DYNAMIC</td>
<td>Gi0/3+Efp</td>
</tr>
</tbody>
</table>
Enabling EoMPLS

You can disable MAC address learning on a VLAN or a bridge domain.
This command disables MAC address learning on a VLAN.

```
Switch(config)# no mac address-table learning vlan 100
```

This command disables MAC address learning on a bridge domain.

```
Switch(config)# no mac address-table learning bridge-domain 100
```

**Note**
The output of the `show mac address-table` command does not include the port name for a pseudowire from which a MAC address is learned.

**Configuring EVC Xconnect**

Follow these steps to configure EVC xconnect:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</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 [gigabitethernet</td>
<td>Specifies the GigabitEthernet or Ten Gigabit Ethernet interface to configure.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>port-channel] port-number</td>
</tr>
<tr>
<td>3</td>
<td>switchport mode trunk</td>
<td>Configure the port as a trunk port.</td>
</tr>
<tr>
<td>4</td>
<td>switchport trunk allowed vlan none</td>
<td>Configure the trunk port to have no allowed VLANs.</td>
</tr>
<tr>
<td>5</td>
<td>service instance id ethernet [evc]</td>
<td>Configure an EFP (service instance) and enter service instance configuration mode. Creates a service instance on an interface and</td>
</tr>
<tr>
<td>6</td>
<td>encapsulation [dot1q</td>
<td>Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.</td>
</tr>
<tr>
<td></td>
<td>untagged</td>
<td>priority-tagged</td>
</tr>
<tr>
<td>7</td>
<td>rewrite ingress tag pop {1/2} symmetric</td>
<td>Specifies the tag manipulation that is to be performed on the frame ingress to the service instance.</td>
</tr>
<tr>
<td>8</td>
<td>xconnect peer-id vc-id [encapsulation</td>
<td>pw-class] [mpls] [pw-class name]</td>
</tr>
<tr>
<td>9</td>
<td>backup peer-id vc-id</td>
<td>Specifies a redundant peer for a pseudowire virtual circuit.</td>
</tr>
</tbody>
</table>

**Configure Pseudowire-class**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>pseudowire-class name</td>
<td>Creates a pseudowire class and enters pseudowire class configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>encapsulation mpls</td>
<td>Specifies the encapsulation type.</td>
</tr>
<tr>
<td>4</td>
<td>interworking [ethernet</td>
<td>vlan</td>
</tr>
</tbody>
</table>
This example shows how to configure EVC Xconnect:

interface GigabitEthernet0/2
switchport trunk allowed vlan none
switchport mode trunk
service instance 1 ethernet
  encapsulation dot1q 10
  xconnect 1.1.1.1 10 encapsulation mpls

service instance 2 ethernet
  encapsulation dot1q 20 cos 5
  xconnect 1.1.1.1 2000 encapsulation mpls

service instance 3 ethernet
  encapsulation dot1q 30 cos 2 etype ipv4
  xconnect 1.1.1.1 350 encapsulation mpls

service instance 4 ethernet
  encapsulation dot1q 40
  rewrite ingress tag pop 1 symmetric
  xconnect 1.1.1.1 415 encapsulation mpls

service instance 5 ethernet
  encapsulation dot1q 50 second-dot1q 60
  xconnect 1.1.1.1 500 encapsulation mpls

service instance 6 ethernet
  encapsulation dot1q 60 second-dot1q 70 cos 5
  xconnect 1.1.1.1 655 encapsulation mpls

service instance 7 ethernet
  encapsulation dot1q 80 second-dot1q 90
  rewrite ingress tag pop 1 symmetric
  xconnect 1.1.1.1 900 encapsulation mpls

service instance 8 ethernet
  encapsulation untagged
  xconnect 1.1.1.1 1000 encapsulation mpls
  backup peer 2.2.2.2 1000
end

Configuring Support for Integrated Routing and Bridging (IRB)

IRB enables a user to route a protocol on one group of interfaces and bridge a protocol on separate group of interfaces within a single router. The protocol can be either routed or bridged on a given interface, but not both.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>configure terminal</th>
<th>Enter global configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>interface [gigabitethernet</td>
<td>Configure the port as a trunk port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>port-channel</td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport mode trunk</td>
<td>Configure the trunk port to have no allowed VLANs.</td>
</tr>
<tr>
<td>Step 4</td>
<td>switchport trunk allowed vlan none</td>
<td></td>
</tr>
</tbody>
</table>
### Packet Flow in an EoMPLS Network

Figure 36-5 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. Switch PE1 establishes a tunnel LSP with switch PE2 by using a label advertised with LDP by Router A, which is connected to switch PE1. Switch PE1 then establishes a targeted LDP session to switch PE2 to advertise the virtual-connection label associated with the VC ID. When switch 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 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 switch 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 PE1 port are configured with that internal VLAN, which makes the PE1 port the only possible destination for the packet.

The PE1 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 designated port, where the packet is again examined and encapsulated with the tunnel label and virtual-connection label based on the EoMPLS for that VLAN.
Chapter 36  Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS

Enabling EoMPLS

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 36-6 shows those parts of the network that are vulnerable to an interruption in service.

**Figure 36-6  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 36-6 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 36-7 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 36-7  L2 VPN Network with Redundant Pseudowires and Attachment Circuits**
Enabling EoMPLS

This section includes this information:

- Configuration Guidelines, page 36-41
- Configuring Pseudowire Redundancy, page 36-41
- Forcing a Manual Switchover to the Backup Pseudowire VC, page 36-42
- Monitoring L2VPN Pseudowire Redundancy, page 36-43

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.

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</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>interface interface-id</code></td>
<td>Specify an interface and enter interface configuration mode. The interface on the adjoining router must be on the same VLAN as this router.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>xconnect peer-router-id vcid pw-class pw-class name</code></td>
<td>Bind the attachment circuit to a pseudowire virtual circuit (VC) and enter xconnect configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>backup peer peer-router-ip-address vcid [pw-class pw-class name]</code></td>
<td>Specify a redundant peer for the pseudowire VC. If you do not specify a <code>pw-class name</code>, the value is inherited from the parent.</td>
</tr>
</tbody>
</table>
Enabling EoMPLS

**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
```

This example shows the output of the `show mpls l2transport vc` privileged EXEC command when the primary attachment circuit is up and the backup attachment circuit is available, but not currently selected.

```
Switch# show mpls l2transport vc
Local intf Local circuit Dest address VC ID Status
----------------- ------------------ ------------------ ------------------
Vl20 Eth VLAN 20 10.1.1.2 20 UP
Vl20 Eth VLAN 20 10.1.1.4 20 DOWN
```

**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:

**Command**

```
xconnect backup force-switchover {interface interface-id | peer ip-address voiced}
```

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>xconnect backup force-switchover {interface interface-id</td>
<td>peer ip-address voiced}</td>
</tr>
</tbody>
</table>

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 36-3 to verify or monitor pseudowire redundancy.

Table 36-1 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>
<tr>
<td>show vfi vfi-name</td>
<td>Display information about a VPLS VFI.</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.

This example shows pseudowire redundancy.

```
Switch# show mpls l2transport vc 10

Local intf  Local circuit              Dest address    VC ID  Status
-------------  -------------------------- --------------- ---------- ----------
Vl10           Eth VLAN 10                1.1.1.1         10         UP
Vl10           Eth VLAN 10                2.2.2.2         10         DOWN
```

Routed VPLS/EoMPLS

Routed VPLS/EoMPLS provides the ability to route or bridge frames to and from pseudowires with MPLS encapsulation. Routed VPLS/EoMPLS accomplishes this by allowing cross-connect and IP addresses to be configured on an SVI.

- Multicast routing is not supported on Routed VPLS

Routed VPLS/EoMPLS supports:

- P2P (SVI based EoMPLS)
- Multi-Point (VPLS)

The following features are supported on routed Routed PW/VPLS:

- SVI based routed pseudowire
- Routed VPLS
- Routed pseudowire over FRR
- L2 multicast over routed pseudowire/VPLS

Figure 36-8 shows how Routed VPLS/EoMPLS is connected.
Configuring Routed Pseudowire

In the privileged EXEC mode, perform these steps to configure routed pseudowire.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1  configure terminal</td>
<td>Enter the global configuration mode.</td>
</tr>
<tr>
<td>Step 2  interface interface-id</td>
<td>Specify the address of the client that will receive the configuration file.</td>
</tr>
<tr>
<td>Step 3  ip address address mask</td>
<td>Specify the IP address and mask for the interface.</td>
</tr>
<tr>
<td>Step 4  xconnect peer-router-id vcid pw-class pw-class name</td>
<td>Bind the attachment circuit to a pseudowire virtual circuit (VC) and enter the Xconnect configuration mode.</td>
</tr>
<tr>
<td>Step 5  end</td>
<td>Return to the privileged EXEC mode.</td>
</tr>
</tbody>
</table>

This is an example of routed pseudowire configuration:

Router#config t
Router(config)#interface vlan333
Router(config-if)#ip address 2.1.1.1 255.255.255.0
Router(config-if)#xconnect 76.76.76.76 105 encapsulation mpls
Router(config-if-xconn)#end

Router#show ip int br | i Vlan333|Interface
<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OK?</th>
<th>Method</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan333</td>
<td>2.1.1.1</td>
<td>YES</td>
<td>manual</td>
<td>up</td>
<td>up</td>
</tr>
</tbody>
</table>

Router#
Configuring Routed VPLS

In the privileged EXEC mode, perform these steps to configure routed VPLS.

<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 the global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>l2 vfi vfi_name manual</td>
<td>Create a virtual forwarding infrastructure (VFI) and enter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>manual VFI configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>vpn id id</td>
<td>Configure the virtual private network (VPN) number for a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VFI interface.</td>
</tr>
<tr>
<td>4</td>
<td>neighbor ip-addr encapsulation mpls</td>
<td>Configure the IP address of the remote peer to become a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>member of the VPLS configured by the VFI and set the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MPLS encapsulation type.</td>
</tr>
<tr>
<td>5</td>
<td>interface interface-id</td>
<td>Specify the address of the client that will receive the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>configuration file.</td>
</tr>
<tr>
<td>6</td>
<td>ip address address mask</td>
<td>Specify the IP address and mask for the interface.</td>
</tr>
<tr>
<td>7</td>
<td>xconnect vfi vfi-name</td>
<td>Bind the attachment circuit to a pseudowire virtual circuit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(VC) and enter the Xconnect configuration mode.</td>
</tr>
<tr>
<td>8</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

This is an example of basic routed VPLS configuration:

```
l2 vfi test manual
vpn id 600
neighbor 10.1.255.2 encapsulation mpls
neighbor 10.1.255.10 encapsulation mpls

interface vlan600
ip address 70.1.1.1 255.255.255.0
xconnect vfi test
```

Support for H-VPLS

The Metro 3800X and Metro 3600X switches support hierarchical VPLS (H-VPLS).

This feature requires the ME 3800X Metro Aggregation Access or ME 3800S Scaled Metro Aggregation Access software license.

H-VPLS uses spoke connections, usually between Layer 2 switches acting as the CE and PE devices at the service provider’s point-of-presence (POP). The spoke connections can be either an IEEE 802.1Q tagged connection or an MPLS LSP.
Figure 36-9 shows two Metro 3800X or Metro 3600X customer-located equipment (CLE) switches (PE1 and PE2) configured as neighbors on different sides of an MPLS network. Each switch has multiple customer Ethernet switches connected to it and is connected to a PE device at the service-provider POP. With no direct connections, H-VPLS allows the customer switches from PE1 to connect to customer switches connected to PE2.

Full-Mesh Configuration

A full-mesh configuration requires a full mesh of tunnel label switched paths (LSPs) between all the PEs that participate in the VPLS. With full mesh, signaling overheads and packet replication requirements for each provisioned VC on a PE can be high.

Set up a VPLS by first creating a virtual forwarding instance (VFI) on each participating PE router. The VFI specifies the VPN ID of a VPLS domain, the addresses of other PE routers in the domain, and the type of tunnel signaling and encapsulation mechanism for each peer PE router.

The set of VFIs formed by the interconnection of the emulated VCs is called a VPLS instance. It is the VPLS instance that forms the logic bridge over a packet-switched network. The VPLS instance is assigned a unique VPN ID.

The PE routers use the VFI to establish a full-mesh LSP of emulated VCs to all the other PE routers in the VPLS instance. PE routers obtain the membership of a VPLS instance through static configuration using the Cisco IOS CLI.

A full-mesh configuration allows the PE router to maintain a single broadcast domain. Thus, when the PE router receives a broadcast, multicast, or unknown unicast packet on an attachment circuit, it sends the packet out through all the other attachment circuits and emulated circuits to all the other CE devices participating in that VPLS instance. The CE devices see the VPLS instance as an emulated LAN.

To avoid the problem of a packet looping in the provider core, the PE devices enforce a split-horizon principle for the emulated VCs. This means that if a packet is received on an emulated VC, it is not forwarded on any other emulated VC.

After the VFI is defined, it must be bound to an attachment circuit, then to the CE device.

The packet forwarding decision is made by looking up the Layer 2 VFI of a particular VPLS domain.
A VPLS instance on a particular PE router receives Ethernet frames that enter on specific physical or logical ports and populate a MAC table that is similar to the way an Ethernet switch works. The PE router can use the MAC address to switch those frames into the appropriate LSP for delivery to the another PE router at a remote site.

If the MAC address is not in the MAC address table, the PE router replicates the Ethernet frame and floods it to all the logical ports associated with that VPLS instance, except the ingress port it just entered. The PE router updates the MAC table as it receives packets on specific ports, and removes the addresses that have not been used for specific periods.

### Hub and Spoke

In a hub-and-spoke model, the PE router that acts as the hub establishes a point-to-multipoint forwarding relationship with all the PE routers at the spoke sites. An Ethernet or VLAN packet received from the customer network on the hub PE can be forwarded to one or more emulated VCs.

The PE routers that act as spokes establish a point-to-point connection to the PE at the hub site. Ethernet or VLAN packets received from the customer network on the spoke PE are forwarded to the VFI or VPLS instance at the hub. If there are a number of customer sites connecting to the spokes, you can terminate multiple VCs per spoke in the same VFI or VPLS instance at the hub.

### VPLS-Supported Features

- **Imposition VLAN rewrite per pseudowire**—This feature connects two L2 domains. VLAN rewrite is usually done at the disposition router. However some devices do not have this capability.
  
  VLAN rewrite at imposition is supported, but with the following restrictions:
  - The rewritten VLANs must be the same if multiple ACs are attached to the same pseudowire
  - Only two VLANS can be written when combining the outer and inner VLANs.
  - All PW inner headers will have the same EtherType.

- **AToM control word per pseudowire**—This feature inserts a control word on a per pseudowire basis. The control word is always set to 0 and does not support any sequencing scheme.

- **PW QoS**—This feature is provided by configuring an input and output policy map on a UNI or PW interface.

- **PW statistics**—This feature provides statistics on packets, bytes, and drops per PW prior to label imposition for packets entering a tunnel and after MPLS disposition for packets exiting a tunnel.

- **UNI to PW mapping for service selection**—This feature allows the following UNI attributes to be used for service selection using port mode EoMPLS and EFP-based EoMPLS:
  - Per UNI port
  - Per UNI port, per C-VLAN
  - Per UNI port, per C-VLAN, per C-CoS
  - Per UNI port, per C-VLAN, per C-DSCP

- **Auto sense signalling**—This feature allows two remote PEs to negotiate VC-type signaling. In earlier software release, two types of VCs were defined, Ethernet VLAN and Ethernet. Only Ethernet is applicable now.

- **Pseudowire over TE tunnel**—This feature allows PW to go over the TE tunnels in which LDP is enabled over the TE tunnel interface and the tunnels are configured end-to-end.
Support for H-VPLS

- Pseudowire over FRR path—This feature allows PW to go over the FRR path.
- PW path selection over Equal-cost routes—This feature allows PWs to be routed over different paths in order to distribute the traffic load.
- LDP MAC address withdrawal—To support faster convergence times, remove and relearn the MAC addresses that have been learned over pseudowire. The LDP Address withdrawal Message contains a list of the MAC address entries that have to be relearned. The message is sent on the backup link to the remote PEs in the VPLS domain.

VPLS Services

Transparent LAN Service (TLS) and Ethernet Virtual Connection Service (EVCS) are available for service providers and enterprises.

- TLS—Use when you need transparency with regard to bridging protocols (for example, bridge protocol data units [BPDUs]) and VLAN values. Bridges see this service as an Ethernet segment.
- EVCS—Use when you need routers to reach multiple intranet and extranet locations from a single physical port. Routers see subinterfaces through which they access other routers.

Transparent LAN Service

TLS is an extension of point-to-point port-based EoMPLS. With TLS, the PE router forwards all the Ethernet packets received from the customer-facing interface (including tagged, untagged, and BPDUs) as follows:

- To a local Ethernet interface or an emulated VC if the destination MAC address is found in the Layer 2 forwarding table.
- To all other local Ethernet interfaces and emulated VCs belonging to the same VPLS domain if the destination MAC address is a multicast or broadcast address or if the destination MAC address is not found in the Layer 2 forwarding table.

Configuring the VPLS Pseudowire

To configure a VPLS pseudowire tunnel between two PE routers, use either of the following procedures:

- Configuring a VPLS Pseudowire Using VFI, page 36-49
- Configuring the Pseudowire Using Pseudowire Class, page 36-33
Configuring a VPLS Pseudowire Using VFI

Create a virtual circuit (VC) using VC Type 5 signaling on each provider edge (PE) router. The interface must be a routed interface or a switched virtual interface (SVI). To establish a bidirectional label-switched protocol (LSP), perform the configuration on both the PE routers. The VC ID is used by both the PE routers to identify a VC.

In the global configuration mode, perform these steps to create a virtual forwarding infrastructure (VFI).

<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>l2 vfi name manual</td>
</tr>
<tr>
<td>Step 3</td>
<td>vpn id vc-id</td>
</tr>
</tbody>
</table>
| Step 4  | neighbor remote router id [vc-id-value] {encapsulation mpls}[no-split-horizon] | Specifies the remote peering router ID and the tunnel encapsulation type or the pseudowire property to be used to set up the emulated VC.  
**Note** Split horizon is the default configuration to avoid broadcast packet looping and to isolate Layer 2 traffic. Use the `no-split-horizon` keyword to disable split horizon and to configure multiple VCs per spoke on the same VFI.  
**Note** The optional VC ID value identifies the emulated VC between a pair of peering PE routers. |
| Step 5  | end | Return to the privileged EXEC mode. |

Configuring a P2P Pseudowire Using pw-class

In the privileged EXEC mode, perform these steps to configure a P2P pseudowire using pw-class:

<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>pseudowire-class pw-class-name manual</td>
</tr>
<tr>
<td>Step 3</td>
<td>encapsulation [mpls]</td>
</tr>
</tbody>
</table>
| Step 4  | interworking {ethernet | ip} | Specifies that Ethernet is used as the interworking interface.  
**Note** The `ip` keyword is not supported in Release 15.1(2)EY. |
| Step 5  | end | Return to the privileged EXEC mode. |

VPLS Autodiscovery: BGP Based

VPLS Autodiscovery enables each Virtual Private LAN Service (VPLS) provider edge (PE) router to discover which other PE routers are part of the same VPLS domain. VPLS Autodiscovery also automatically detects when PE routers are added to or removed from the VPLS domain. You no longer
Support for H-VPLS

need to manually configure the VPLS and maintain the configuration when a PE router is added or deleted. VPLS Autodiscovery uses the Border Gateway Protocol (BGP) to discover the VPLS members and to set up and tear down pseudowires in the VPLS.

Information About VPLS Autodiscovery: BGP Based

To understand VPLS Autodiscovery, you should understand the following concepts:

- How the VPLS Feature Works, page 36-50
- How the VPLS Autodiscovery: BGP Based Feature Works, page 36-50
- How Enabling VPLS Autodiscovery Differs from Manually Configuring VPLS, page 36-50
- Show Commands Affected by VPLS Autodiscovery: BGP Based, page 36-51

How the VPLS Feature Works

VPLS allows Multiprotocol Label Switching (MPLS) networks to provide multipoint Ethernet LAN services, also known as Transparent LAN Services (TLS). All customer sites in a VPLS appear to be on the same LAN, even though those sites might be in different geographic locations.

How the VPLS Autodiscovery: BGP Based Feature Works

VPLS Autodiscovery enables each VPLS PE router to discover the other PE routers that are part of the same VPLS domain. VPLS Autodiscovery also tracks when PE routers are added to or removed from the VPLS domain. The autodiscovery and signaling functions use BGP to find and track the PE routers.

BGP uses the L2VPN Routing Information Base (RIB) to store endpoint provisioning information, which is updated each time any Layer 2 VFI is configured. Prefix and path information is stored in the L2VPN database, allowing BGP to make decisions on the best path. When BGP distributes the endpoint provisioning information in an update message to all its BGP neighbors, the endpoint information is used to configure a pseudowire mesh to support L2VPN-based services.

The BGP autodiscovery mechanism facilitates the configuration of L2VPN services, which are an integral part of the Cisco IOS Virtual Private LAN Service (VPLS) feature. VPLS enables flexibility in deploying services by connecting geographically dispersed sites as a large LAN over high-speed Ethernet in a robust and scalable IP MPLS network. For more information about BGP and the L2VPN address family in relation to VPLS Autodiscovery, see the following documents:

- The section called “L2VPN Address Family” in the Cisco BGP Overview.
- The document called BGP Support for the L2VPN Address Family

How Enabling VPLS Autodiscovery Differs from Manually Configuring VPLS

With VPLS Autodiscovery, you no longer need to manually set up the VPLS. The commands you use to set up VPLS Autodiscovery are similar to those you use to manually configure a VPLS, as shown in Table 2. VPLS Autodiscovery uses neighbor commands in L2VPN address family mode to distribute endpoint information to configure a pseudowire.
When you configure VPLS Autodiscovery, you enter the `l2vfi autodiscovery` command. This command allows the VFI to learn and advertise the pseudowire endpoints. As a result, you no longer need to enter the `neighbor (VPLS)` command in L2 VFI configuration mode.

However, the `neighbor (VPLS)` command is still supported with VPLS Autodiscovery in L2 VFI command mode. You can use the `neighbor (VPLS)` command to allow PE routers that do not participate in the autodiscovery process to join the VPLS. You can also use the `neighbor (VPLS)` command with PE routers that have been configured using the Tunnel Selection feature. You can also use the `neighbor (VPLS)` command in hierarchical VPLS configurations that have U-PE routers that do not participate in the autodiscovery process and have split-horizon forwarding disabled.

**Show Commands Affected by VPLS Autodiscovery: BGP-Based**

VPLS Autodiscovery changes the following show commands:

- The `show mpls l2transport vc` command with the `detail` keyword has been updated to include FEC 129 signaling information for the autodiscovered VPLS pseudowires.
- The `show vfi` command now displays information related to autodiscovered VFIs. The new information includes the VPLS ID, the route distinguisher (RD), the RT, and the router IDs of the discovered peers.
- The `show xconnect` command has been updated with the `rib` keyword to provide RIB information about the pseudowires.

**How to Configure VPLS Autodiscovery: BGP-Based**

To configure VPLS Autodiscovery, perform the following tasks:

- Enabling VPLS Autodiscovery: BGP-Based, page 36-52 (required)
- Configuring BGP to Enable VPLS Autodiscovery, page 36-52 (required)
- Customizing the VPLS Autodiscovery Settings, page 36-54 (optional)
Enabling VPLS Autodiscovery: BGP Based

Perform the following task to enable each VPLS PE router to discover the other PE routers that are part of the same VPLS domain.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> l2 vfi vfi-name autodiscovery</td>
<td>Enables VPLS Autodiscovery on the PE router and enters L2 VFI configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> vpn id vpn-id</td>
<td>Configures a VPN ID for the VPLS domain.</td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits L2 VFI configuration mode. Commands take effect after the router exits L2 VFI configuration mode.</td>
</tr>
</tbody>
</table>

Configuring BGP to Enable VPLS Autodiscovery

BGP learns the endpoint provisioning information from the L2VPN database which is updated each time a Layer 2 virtual forwarding instance (VFI) is configured. When BGP distributes the endpoint provisioning information in an update message to all its BGP neighbors, the endpoint information is used to configure a pseudowire mesh to support aL2VPN-based services.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> router bgp autonomous-system-number</td>
<td>Enters router configuration mode for the specified routing process.</td>
</tr>
<tr>
<td><strong>Step 4</strong> no bgp default ipv4-unicast</td>
<td>Disables the IPv4 unicast address family for the BGP routing process.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Routing information for the IPv4 unicast address family is advertised by default for each BGP routing session configured with the neighbor remote-as router configuration command unless you configure the no bgp default ipv4-unicast router configuration command before configuring the neighbor remote-as command. Existing neighbor configurations are not affected.</td>
</tr>
<tr>
<td><strong>Step 5</strong> bgp log-neighbor-changes</td>
<td>Enables logging of BGP neighbor resets.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 6 | `neighbor (ip-address | peer-group-name) remote-as autonomous-system-number` | Adds the IP address or peer group name of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router.  
- If the `autonomous-system-number` argument matches the autonomous system number specified in the `router bgp` command, the neighbor is an internal neighbor.  
- If the `autonomous-system-number` argument does not match the autonomous system number specified in the `router bgp` command, the neighbor is an external neighbor.  
- In this example, the neighbor at 10.10.10.1 is an internal BGP neighbor. |
| Step 7 | `neighbor (ip-address | peer-group-name) update-source interface-type interface-number` | (Optional) Configures a router to select a specific source or interface to receive routing table updates.  
- This example uses a loopback interface. The advantage to this configuration is that the loopback interface is not affected by the effects of a flapping interface. |
| Step 8 | Repeat Step 6 and Step 7 to configure other BGP neighbors | — |
| Step 9 | `address-family l2vpn [vpls]` | Specifies the L2VPN address family and enters address family configuration mode.  
- The optional `vpls` keyword specifies that VPLS endpoint provisioning information is to be distributed to BGP peers.  
- In this example, an L2VPN VPLS address family session is created. |
| Step 10 | `neighbor (ip-address | peer-group-name) activate` | Enables the neighbor to exchange information for the L2VPN VPLS address family with the local router. |
| Step 11 | `neighbor (ip-address | peer-group-name) send-community (both | standard | extended)` | Specifies that a communities attribute should be sent to a BGP neighbor.  
- In this example, an extended communities attribute is sent to the neighbor at 10.10.10.1. |
| Step 12 | Repeat Step 10 and Step 11 to activate other BGP neighbors under an L2VPN address family. | — |
| Step 13 | `exit-address-family` | Exits address family configuration mode and returns to router configuration mode. |
| Step 14 | `exit` | Exits router configuration mode. |
| Step 15 | `exit` | Exits privileged EXEC mode. |
| Step 16 | `show vfi` | (Optional) Displays information about the configured VFI instances. |
| Step 17 | `show ip bgp l2vpn vpls (all | rd vpn-rd)` | (Optional) Displays information about the Layer2 VPN VPLS address family. |
Chapter 36 Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS

Support for H-VPLS

Customizing the VPLS Autodiscovery Settings

Several commands allow you to customize the VPLS environment. You can specify identifiers for the VPLS domain, the route distinguisher, the route target, and the PE router. Perform the following steps to customize these settings.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3 l2 vfi vfi-name autodiscovery</td>
<td>Enables VPLS Autodiscovery on the PE router and enters L2 VFI configuration mode.</td>
</tr>
<tr>
<td>Step 4 vpn id vpn-id</td>
<td>Configures a VPN ID for the VPLS domain.</td>
</tr>
<tr>
<td>Step 5 vpls-id {autonomous-system-number:nn</td>
<td>(Optional) Specifies the VPLS domain. This command is optional, because VPLS Autodiscovery automatically generates a VPLS ID using the BGP autonomous system number and the configured VFI VPN ID. You can use this command to change the automatically generated VPLS ID.</td>
</tr>
<tr>
<td>Step 6 rd {autonomous-system-number:nn</td>
<td>(Optional) Specifies the RD to distribute endpoint information. This command is optional, because VPLS Autodiscovery automatically generates an RD using the BGP autonomous system number and the configured VFI VPN ID. You can use this command to change the automatically generated route distinguisher.</td>
</tr>
<tr>
<td>Step 7 route-target [import</td>
<td>export</td>
</tr>
</tbody>
</table>
VPLS Autodiscovery: BGP Based: Basic Example

Figure 10 show a basic configuration of VPLS Autodiscovery.

**Figure 10  Basic VPLS Autodiscovery Configuration**

![Basic VPLS Autodiscovery Configuration Diagram]

**PE1**

```plaintext
12 router-id 10.1.1.1
12 vfi auto autodiscovery
  vpn id 100
! pseudowire-class mpls
  encapsulation mpls
! interface Loopback1
  ip address 10.1.1.1 255.255.255.255
! interface Ethernet0/0
```
Support for H-VPLS

Chapter 36 Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS

description Backbone interface
ip address 192.168.0.1 255.255.255.0
mpls ip
!
router ospf 1
log-adjacency-changes
network 10.1.1.0 0.0.0.255 area 0
network 10.16.0.0 0.0.0.255 area 0
!
router bgp 1
no bgp default ipv4-unicast
bgp log-neighbor-changes
bgp update-delay 1
neighbor 10.1.1.2 remote-as 1
neighbor 10.1.1.2 update-source Loopback1
neighbor 10.1.1.3 remote-as 1
neighbor 10.1.1.3 update-source Loopback1
!
address-family ipv4
no synchronization
no auto-summary
exit-address-family
!
address-family l2vpn vpls
neighbor 10.1.1.2 activate
neighbor 10.1.1.2 send-community extended
neighbor 10.1.1.3 activate
neighbor 10.1.1.3 send-community extended
exit-address-family

PE2

l2 router-id 10.1.1.2
l2 vfi auto autodiscovery
vpn id 100
!
pseudowire-class mpls
encapsulation mpls
!
interface Loopback1
ip address 10.1.1.2 255.255.255.255
!
interface Ethernet0/0
description Backbone interface
ip address 192.168.0.2 255.255.255.0
mpls ip
!
router ospf 1
log-adjacency-changes
network 10.1.1.0 0.0.0.255 area 0
network 10.16.0.0 0.0.0.255 area 0
!
router bgp 1
no bgp default ipv4-unicast
bgp log-neighbor-changes
bgp update-delay 1
neighbor 10.1.1.1 remote-as 1
neighbor 10.1.1.1 update-source Loopback1
neighbor 10.1.1.3 remote-as 1
neighbor 10.1.1.3 update-source Loopback1
!
address-family ipv4
no synchronization
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 switch supports these MPLS OAM features:

- LSP ping/traceroute LDP IPv4 version 3
Understanding MPLS OAM

- 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).
- 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 33, “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 module 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 15.1(2)EY.”

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.

The switch supports IP load balancing, up to a total of four next-hop paths. With the IP license, the switch supports up to sixteen next-hop paths. Each path supports up to four Equal Cost Routing (ECR) multipaths.

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/ipsla/configuration/guide/sla_lsp_mon_autodisc.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.
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 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 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 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 OAM on a switch:

- Default MPLS OAM Configuration, page 36-61
- MPLS OAM Configuration Guidelines, page 36-61

These sections describe the optional or required tasks:

- Using LSP Ping for LDP IPv4 FEC, page 36-62
- Using LSP Ping to Specify a MPLS TE Tunnel, page 36-64
- Using LSP Traceroute, page 36-65
- Using LSP Ping for Pseudowire (AToM VCCV), page 36-67
- Configuring IP SLAs MPLS Ping and Traceroute, page 36-69
- Using LSP Tree Trace, page 36-75

### 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:

- 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 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.
## 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>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping mpls ipv4</td>
<td>Configure LSP IPv4 ping. The keywords have these meanings:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>destination-address</code></td>
<td>• <code>destination-address</code>—Specify the address and network mask of the target FEC.</td>
</tr>
<tr>
<td></td>
<td><code>destination-mask</code></td>
<td>• (Optional) <code>destination address-start address-end increment</code>—Enter the destination 127 network address range.</td>
</tr>
<tr>
<td></td>
<td><code>exp exp-bits</code></td>
<td>• (Optional) <code>exp exp-bits</code>—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><code>interval ms</code></td>
<td>• (Optional) <code>interval ms</code>—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><code>pad pattern</code></td>
<td>• (Optional) <code>pad pattern</code>—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><code>repeat count</code></td>
<td>• (Optional) <code>repeat count</code>—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><code>reply dscp dscp-value</code></td>
<td>• (Optional) <code>reply dscp dscp-value</code>—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><code>interval ms</code></td>
<td>• (Optional) <code>interval ms</code>—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><code>pad pattern</code></td>
<td>• (Optional) <code>pad pattern</code>—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><code>repeat count</code></td>
<td>• (Optional) <code>repeat count</code>—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><code>reply dscp dscp-value</code></td>
<td>• (Optional) <code>reply dscp dscp-value</code>—Specify a specific class of service (CoS) in an echo reply by providing a differentiated services code point (DSCP) value.</td>
</tr>
</tbody>
</table>
This is an example of an LSP IPv4 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 Ping to Specify a MPLS TE Tunnel

To specify the destination type as an MPLS traffic engineering (TE) tunnel and tunnel interface, use the `ping mpls traffic-eng` privileged EXEC command.

Beginning in privileged EXEC mode, follow these steps to specify the destination type as an MPLS TE tunnel and interface:

### Command
```
Step 1  ping mpls traffic-eng {tunnel intf num} [dsmap] [exp exp bits in MPLS header]
       [force-explicit-null] [interval send interval between requests in msec]
       [pad pad TLV pattern] [repeat repeat count] [reply dscp differentiated services codepoint value]
       [reply mode {ipv4 | router-alert | no-reply | reply pad-tlv}] [revision echo packet tlv versioning]
       [source source specified as an IP address] {sweep {min value | max value} {increment} | [timeout send interval between requests in msec] [ttl time-to-live] [verbose]}
```

### Purpose
Specify the destination type as an MPLS TE tunnel and interface. The keywords have these meanings:

- **tunnel intf num**—Specifies the destination type as an MPLS traffic engineering (TE) tunnel and the tunnel interface number. The range for the tunnel interface number is from 0 to 65535.
- **dsmap**—Indicates that a downstream mapping (DSMAP) type length and value should be included in the LSP echo request.
- **exp exp bits in MPLS header**—Specifies the MPLS experimental field value in the MPLS header for echo replies. Range is 0 to 7. Default is 0.
- **force-explicit-null**—Forces an unsolicited explicit null label to be added to the MPLS label stack and allows LSP ping to be used to detect LSP breakages at the penultimate hop.
- **interval send interval between requests in msec**—Specifies a send interval between requests in milliseconds. The range is 0 to 3600000 ms; the default is 0 (no interval is configured).
- **pad pad tlv pattern**—Specifies the pad pattern for an echo request.
- **repeat repeat count**—Specifies the number of times to resend the packet. The range is from 1 to 2147483647. If you do not enter the repeat keyword, the packet is sent 5 times.
### Configuring MPLS OAM and IP SLAs MPLS

#### Using LSP Traceroute

To learn the routes that packets follow when travelling to their destinations, use the `traceroute mpls` command in EXEC mode.

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 traceroute:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Configure LSP traceroute. The keywords have these meanings:</td>
</tr>
<tr>
<td></td>
<td>• <strong>ipv4 addr/mask</strong>—Specifies the destination type as a LDP prefix. Enter the address prefix of the target and number of bits in the target address network mask.</td>
</tr>
<tr>
<td></td>
<td>• <strong>traffic-eng tunnel tunnel intf num</strong>—Specifies the destination type as an MPLS traffic engineering (TE) tunnel and tunnel interface.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) <strong>destination {start address} {end address} {address increment}</strong>—Specifies a network 127 address to be used as the destination address in the echo request packet.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) <strong>exp exp bits in MPLS header</strong></td>
</tr>
<tr>
<td></td>
<td>• Forces an unsolicited explicit NULL label to be added to the MPLS label stack and allows LSP ping to be used to detect LSP breakages at the penultimate hop.</td>
</tr>
<tr>
<td></td>
<td>• Specifies the output interface where echo request packets are sent.</td>
</tr>
<tr>
<td></td>
<td>• Specifies the differentiated service codepoint value for an MPLS echo reply.</td>
</tr>
<tr>
<td></td>
<td>• Specifies the reply mode for the echo request packet. Enter <strong>ipv4</strong> to reply with an IPv4 UDP packet (the default) or <strong>router-alert</strong> to reply with an IPv4 UDP packet with router alert.</td>
</tr>
<tr>
<td></td>
<td>• Specifies the Cisco extension TLV versioning field:</td>
</tr>
<tr>
<td></td>
<td>– 1 draft-ietf-mpls-lsp-ping-03 (initial)</td>
</tr>
<tr>
<td></td>
<td>– 2 draft-ietf-mpls-lsp-ping-03 (rev 1)</td>
</tr>
<tr>
<td></td>
<td>– 3 draft-ietf-mpls-lsp-ping-03 (rev 2)</td>
</tr>
<tr>
<td></td>
<td>– 4 draft-ietf-mpls-lsp-ping-09 (initial)</td>
</tr>
<tr>
<td></td>
<td>• Specifies the source address used in the echo request packet.</td>
</tr>
<tr>
<td></td>
<td>• Specifies the timeout interval in seconds. Range is from 0 to 3600. Default is 2 seconds.</td>
</tr>
<tr>
<td></td>
<td>• Specifies the maximum number of hops. The range is from 1 to 255.</td>
</tr>
<tr>
<td></td>
<td>• Enables verbose output information, including MPLS echo reply, sender address of the packet, and return codes.</td>
</tr>
</tbody>
</table>
Here are some examples 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
Switch# traceroute mpls traffic-eng tunnel 4

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>
</table>
| **Step 1** ping mpls pseudowire ipv4-address vc-id [destination start-address [end-address [address-increment]]] [exp exp-bits] [interval ms] [pad pattern] [repeat count] [reply dscp dscp-value] [reply mode {ipv4 | router-alert}] [revision {1 | 2 | 3}] [size packet-size] [source source-address] [sweep minimum maximum size-increment] [timeout seconds] [verbose] [dsmap [hashkey {none | ipv4 bitmap bitmap-size} [flags fec] | Configure LSP ping over pseudowire. The keywords have these meanings:

- **ipv4-address**—Specify the IPv4 address of the peer.
- **vc-id**—Specify virtual-circuit identification number. The range is from 1 to 4294967295.
- **(Optional) destination**—Enter the destination 127 network address or address range with increment.
- **(Optional) exp exp-bits**—Specify the MPLS experimental-field value in the MPLS header. The range is from 0 to 7. The default is 0.
- **(Optional) interval ms**—Specify the time in milliseconds between successive MPLS echo requests. The range is from 0 to 3600000; the default is 0.
- **(Optional) pad pattern**—Specify that the pad TLV is used to fill the datagram so that the MPLS echo request is the specified size.
- **(Optional) 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.
- **(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.
- **(Optional) 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.
- **(Optional) revision**—Enter the IETF MPLS ping draft revision number as 1, 2, or 3.
- **(Optional) 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.
- **(Optional) 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 traceroute 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 36-70
- Manually Configuring IP SLAs MPLS LSP Ping or Traceroute, page 36-73

For more details about LSP Health Monitor and MPLS IP SLAs ping or traceroute, see the IP SLAs - LSP Health Monitor configuration guide at this URL:


For more details about IP SLAs operations, see Chapter 36, “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>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>auto ip sla mpls-lsp-monitor operation-number</td>
</tr>
<tr>
<td>Step 3</td>
<td>type {echo</td>
</tr>
<tr>
<td></td>
<td>• echo—Select an LSP monitor ping operation.</td>
</tr>
<tr>
<td></td>
<td>• pathEcho—Select an LSP monitor traceroute operation.</td>
</tr>
<tr>
<td></td>
<td>• ipsla-vrf-all—Configure IP SLAs MPLS LSP monitor for all VPNs.</td>
</tr>
<tr>
<td></td>
<td>• vrf vpn-name—Configure the IP SLAs LSP monitor for the specified VPN.</td>
</tr>
<tr>
<td>Step 4</td>
<td>access-list access-list-number</td>
</tr>
<tr>
<td>Step 5</td>
<td>delete-scan-factor factor</td>
</tr>
<tr>
<td></td>
<td>Note You must use the scan-interval command with this command.</td>
</tr>
<tr>
<td>Step 6</td>
<td>exp exp-bits</td>
</tr>
<tr>
<td>Step 7</td>
<td>force-explicit-null</td>
</tr>
<tr>
<td>Step 8</td>
<td>lsp-selector ip-address</td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Step 9 reply-dscp-bits <code>$dscp-value</code></td>
<td>(Optional) Specify the differentiated services codepoint (DSCP) value for an echo reply packet of an IP SLAs operation. The default value is 0.</td>
</tr>
<tr>
<td>Step 10 reply-mode `{ipv4</td>
<td>router-alert}`</td>
</tr>
<tr>
<td>Step 11 request-data-size <code>$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>Step 12 scan-interval <code>$minutes</code></td>
<td>(Optional) Specifies the time interval (in minutes) at which the LSP Health Monitor checks the scan queue for BGP next hop neighbor updates. The range is 1 to 70560; the default is 240 minutes.</td>
</tr>
<tr>
<td>Step 13 secondary-frequency `{connection-loss</td>
<td>timeout}<code> </code>$frequency`</td>
</tr>
<tr>
<td>Step 14 tag <code>text</code></td>
<td>(Optional) Create a user-specified identifier for an IP SLAs operation.</td>
</tr>
<tr>
<td>Step 15 threshold <code>$milliseconds</code></td>
<td>(Optional) Specify the rising threshold (hysteresis) that generates a reaction event and stores history information for an IP SLAs operation. The range is 0 to 2147483647; the default is 5000 ms.</td>
</tr>
<tr>
<td>Step 16 timeout <code>$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>Step 17 ttl <code>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>Step 18 exit</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>Step 19 exit</td>
<td>Exit auto IP SLA MPLS parameter configuration mode and returns to global configuration mode.</td>
</tr>
</tbody>
</table>
### Chapter 36      Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS

#### 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 2147483647.</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>
<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>request-data-size &lt;em&gt;bytes&lt;/em&gt;</td>
<td><em>(Optional) Specify the protocol data size for an IP SLAs request packet. The range is 100 to 1500; the default is 100 bytes.</em></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>secondary-frequency &lt;br&gt; {(connection-loss</td>
<td>timeout) &lt;em&gt;frequency&lt;/em&gt;}</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>tag &lt;em&gt;text&lt;/em&gt;</td>
<td><em>(Optional) Create a user-specified identifier for an IP SLAs operation.</em></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>threshold &lt;em&gt;milliseconds&lt;/em&gt;</td>
<td><em>(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.</em></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>timeout &lt;em&gt;milliseconds&lt;/em&gt;</td>
<td><em>(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.</em></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>ttl &lt;em&gt;time-to-live&lt;/em&gt;</td>
<td><em>(Optional) Specify the maximum hop count for an IP SLAs echo request packet. The range is 1 to 255.</em></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>ip sla schedule &lt;br&gt; &lt;em&gt;operation-number&lt;/em&gt; [ageout &lt;br&gt; &lt;em&gt;seconds&lt;/em&gt;] [life {forever</td>
<td>&lt;br&gt; &lt;em&gt;seconds&lt;/em&gt;} ] [recurring] &lt;br&gt; [start-time {hh:mm [:ss]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td>show ip sla configuration [&lt;em&gt;operation-number&lt;/em&gt;]</td>
<td>Show the configured LSP monitoring operations.</td>
</tr>
</tbody>
</table>
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 36-75
- Configuring ECMP IP SLAs Tree Trace, page 36-76

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 | Configure LSP LDP IPv4 traceroute. The keywords have these meanings:
| router-alert]] [revision 1 2 3] [source source-address] [timeout seconds] [ttl time-to-live] [verbose] [revision tlv-revision-number] [force-explicit-null] [output interface interface-id [nexthop ip-address]] [flags fec] | • `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.
Configuring MPLS OAM and IP SLAs MPLS

Chapter 36  Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS

Configuring MPLS OAM and IP SLAs MPLS

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><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>auto ip sla mpls-lsp-monitor operation-number</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>path-discover</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>force-explicit-null</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>hours-or-statistics kept hours</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 SLAs 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.*
### Command and Purpose

**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.
Monitoring and Maintaining MPLS and EoMPLS

To clear MPLS counters or display MPLS and EoMPLS information, use the privileged EXEC commands in Table 36-3.

### Table 36-3 Commands for Displaying MPLS and EoMPLS Information

<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>
<tr>
<td>show mpls l2transport vc [detail] [summary]</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>show mpls l2transport vc [vc-id] [vc-id-min - vc-id-max]</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>show mpls label range</td>
<td>Display the range of local labels available for use on packet interfaces.</td>
</tr>
<tr>
<td>show mpls ldp backoff</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>show mpls ldp bindings</td>
<td>Display the contents of the label information base (LIB).</td>
</tr>
<tr>
<td>show mpls ldp discovery</td>
<td>Display the status of the LDP discovery process.</td>
</tr>
</tbody>
</table>
### Table 36-3  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 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 identify and resolve software problems related to the Cisco IOS software on the Cisco ME 3800X and ME 3600X switch.
You can use the command-line interface (CLI) to identify and solve problems.
Additional troubleshooting information related to hardware 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.

- Recovering from a Lost or Forgotten Password, page 2
  - Note Recovery procedures require that you have physical access to the switch.
- Preventing Autonegotiation Mismatches, page 6
- SFP Module Security and Identification, page 7
- Monitoring SFP Module Status, page 7
- Monitoring Temperature, page 7
- Using Ping, page 8
- Using Layer 2 Traceroute, page 8
- Using IP Traceroute, page 10
- Using TDR, page 37-12
- Using Debug Commands, page 12
- Using the crashinfo File, page 14
- Using On-Board Failure Logging, page 15
Recovering from a Lost or Forgotten Password

The default configuration for the switch allows an end user to recover from a lost password by interrupting the boot process during power-on and by entering a new password.

On these switches, a system administrator can disable some of the functionality of password recovery 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.

Disabling password recovery provides configuration file security by preventing unauthorized users from accessing the configuration file.

The Cisco ME switch boot loader uses break-key detection to stop the automatic boot sequence for the password recovery purpose.

The break key character is different for each operating system.

On a SUN work station running UNIX, Ctrl-C is the break key.

On a PC running Windows XP or 2000, Ctrl-Break is the break key.

Cisco TAC has tabulated break keys for most common operating systems and an alternative break key sequence for those terminal emulators that do not support the break keys. To see that list go to: http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a0080174a34.shtml

These sections describes how to recover a forgotten or lost switch password:
- Procedure with Password Recovery Enabled, page 3
- Procedure with Password Recovery Disabled, page 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.
Reconnect the power cord to the switch.
Step 4 After the switch performs POST, the switch begins the autoboot process. The boot loader prompts the user for a break key character during the boot-up sequence, as shown in this example:

***** The system will autobooot in 5 seconds *****

Send a break key to prevent autoboooting.

You must enter the break key on the console terminal within 5 seconds of receiving the message that the system will autobooot. The System LED flashes green until the break key is accepted. After the break key is accepted, the System LED turns off until after the switch boots.
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, or encountered an error during initialization of the flash filesystem. The following commands will initialize the flash filesystem, and finish loading the operating system software:

```
flash_init
load_helper
boot
```

proceed to the “Procedure with Password Recovery Enabled” section on page 3, 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 5, and follow the steps.

**Step 5** After recovering the password, reload the switch:

```
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, or encountered an error during initialization of the flash filesystem. The following commands will initialize the flash filesystem, and finish loading the operating system software:

```
flash_init
load_helper
boot
```

**Step 1** Initialize the flash file system:

```
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:

```
switch: load_helper
```

**Step 4** Display the contents of flash memory:

```
switch: dir flash:
```

The switch file system appears:

```
Directory of flash:
11 -rwx 5825 Mar 01 1993 22:31:59 config.text
18 -rwx 720 Mar 01 1993 02:21:30 vlan.dat
```
Step 5  Rename the configuration file to config.text.old.  
This file contains the password definition.  
```
switch: rename flash:config.text flash:config.text.old
```

Step 6  Boot the system:  
```
switch: boot
```
You are prompted to start the setup program. Enter \textbf{N} at the prompt:  
```
Continue with the configuration dialog? [yes/no]: \textbf{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
```
Source filename \texttt{[config.text]}?  
Destination filename \texttt{[running-config]}?  
Press \textbf{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.

\textbf{Note}  
This procedure is likely to leave your switch virtual interface in a shutdown state. You can identify this interface by entering the \texttt{show running-config} privileged EXEC command. To re-enable the interface, enter the \texttt{interface vlan} \texttt{vlan-id} global configuration command, and specify the VLAN ID of the shutdown interface. With the switch in interface configuration mode, enter the \texttt{no shutdown} command.
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.

Note

Disabling password recovery provides configuration file security by preventing unauthorized users from accessing the configuration file.

- If you enter n (no), the normal boot process continues as if the break key 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:

Directory of flash:

16128000 bytes total (10003456 bytes free)

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.

---

**Note** This procedure is likely to leave your switch virtual interface in a shutdown state. You can identify this interface 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 10** You must now reconfigure the switch. If the system administrator has the backup switch and VLAN configuration files available, you should use those.

---

**Preventing Autonegotiation Mismatches**

The IEEE 802.3ab autonegotiation protocol manages the switch settings for speed (10, 100, and 1000 Mbps, excluding SFP module ports) 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.
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.

### Monitoring Temperature

The switch monitors the temperature conditions. The switch also uses the temperature information to control the fans. The temperature value is the temperature in the switch (not the external temperature). Enter the `show env temperature` privileged EXEC command to see if the temperature is okay or faulty.

You can use the `show env temperature status` privileged EXEC command to display the temperature value, state, and thresholds. You can configure a high and low threshold level (in Celsius) to generate an alert by using the `system env temperature alert {high | low} value` global configuration command.

The `show env temperature status` command displays the temperature value, state, and thresholds.
These are examples of output from the `show env temperature` and `show env temperature status` commands:

Switch> `show env temperature`
SYSTEM TEMPERATURE is GREEN

Switch> `show env temperature status`
SYSTEM Temperature Value: 35.5 Degree Celsius
SYSTEM Temperature State: GREEN
SYSTEM Low Temperature Alert Threshold: 0.0 Degree Celsius
SYSTEM Low Temperature Shutdown Threshold: -20.0 Degree Celsius
SYSTEM High Temperature Alert Threshold: 58.0 Degree Celsius
SYSTEM High Temperature Shutdown Threshold: 80.0 Degree Celsius
POWER SUPPLY 1 Temperature Value: 32.7500 Degree Celsius
POWER SUPPLY 1 Temperature Alert Threshold: 85.0000 Degree Celsius
POWER SUPPLY 1 Temperature Shutdown Threshold: 110.0000 Degree Celsius
FAN TRAY 2: No Temperature Information Provided

For more information, see the command reference for this release.

### Using 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. To ping a host in a different IP subnetwork from the switch, you must have IP routing configured to route between the subnets, and a static route to the destination might also be appropriate. If you need to enable or configure IP routing, see Chapter 29, “Configuring IP Unicast Routing.”

Beginning in privileged EXEC mode, use the `ping` command to ping another device on the network from the switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`ping [host</td>
<td>address]`</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Though other protocol keywords are available with the <code>ping</code> command, they are not supported in this release.</td>
</tr>
</tbody>
</table>

To end a ping session, simultaneously press and release the `Ctrl`, `Shift`, and `6` keys, and then press the `X` key.

### Using Layer 2 Traceroute

- [Understanding Layer 2 Traceroute](#), page 9
- [Layer 2 Traceroute Usage Guidelines](#), page 9
- [Displaying the Physical Path](#), page 10
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 finds 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.

Note
Layer 2 traceroute is not available only on ports configured with service instances.

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.

Layer 2 Traceroute Usage Guidelines

- Ports configured with service instances do not support Layer 2 traceroute.
- 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. CDP is enabled by default. If any devices in the physical path are transparent to CDP, the switch cannot identify the path through these devices. For more information about enabling CDP, see Chapter 21, “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:

- `traceroute mac [interface interface-id] {source-mac-address} [interface interface-id] {destination-mac-address} [vlan vlan-id] [detail]`
- `traceroute 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

- Understanding IP Traceroute, page 10
- Executing IP Traceroute, page 11

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 output. Intermediate switches do not show up in the 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 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 an Internet Control Message Protocol (ICMP) time-to-live-exceeded message to the source. Traceroute finds the address of the first hop by examining the source address field of this 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 learn 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 that this message was sent by the destination port.

**Executing IP Traceroute**

Beginning in privileged EXEC mode, follow this step to trace that the path packets take through the network:

```
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 171.9.15.10
  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>
<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>

**Table 37-1  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 end a trace in progress, enter the escape sequence (Ctrl-^ X by default). Simultaneously press and release the Ctrl, Shift, and 6 keys, and then press the X key.

Using TDR

- Understanding TDR, page 12
- Running TDR and Displaying the Results, page 12

Understanding TDR

You can use the Time Domain Reflector (TDR) feature to diagnose and resolve cabling problems. When running TDR, a local device sends a signal through a cable and compares the reflected signal to the initial signal.

TDR can detect these cabling problems:

- Open, broken, or cut twisted-pair wires—The wires are not connected to the wires from the remote device.
- Shorted twisted-pair wires—The wires are touching each other or the wires from the remote device. For example, a shorted twisted pair can occur if one wire of the twisted pair is soldered to the other wire.

If one of the twisted-pair wires is open, TDR can find the length at which the wire is open.

Use TDR to diagnose and resolve cabling problems in these situations:

- Replacing a switch
- Setting up a wiring closet
- Troubleshooting a connection between two devices when a link cannot be established or when it is not operating properly

Running TDR and Displaying the Results

To run TDR, enter the test cable-diagnostics tdr interface interface-id privileged EXEC command:

To display the results, enter the show cable-diagnostics tdr interface interface-id privileged EXEC command. For a description of the fields in the display, see the command reference for this release.

Note

ITDR is supported only on the copper Ethernet 10/100/1000 ports.

Using Debug Commands

- Enabling Debugging on a Specific Feature, page 13
- Enabling All-System Diagnostics, page 13
- Redirecting Debug and Error Message Output, page 14
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 all Flex Links backup interface:

```bash
Switch# debug backup all
```

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 that 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 that 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 Flex Links, enter this command in privileged EXEC mode:

```bash
Switch# no debug backup all
```

Alternately, in privileged EXEC mode, you can enter the `undebug` form of the command:

```bash
Switch# undebug backup all
```

To display the state of each debugging option, enter this command in privileged EXEC mode:

```bash
Switch# show debugging
```

Enabling All-System Diagnostics

Beginning in privileged EXEC mode, enter this command to enable all-system diagnostics:

```bash
Switch# debug all
```

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 24, “Configuring System Message Logging.”

### 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 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 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.
Using On-Board Failure Logging

You can use the on-board-failure logging (OBFL) feature to collect information about the switch. The information includes uptime, temperature, and voltage information and helps Cisco technical support representatives to troubleshoot switch problems.

This section has this information:

- Understanding OBFL, page 15
- Configuring OBFL, page 15
- Displaying OBFL Information, page 16

Understanding OBFL

By default, OBFL is enabled and is automatically activated five minutes after the switch boots up. It collects information about the switch and small form-factor pluggable (SFP) modules. The switch stores this information in the flash memory:

- CLI commands—Record of the OBFL CLI commands that are entered on a switch
- Environmental data—Unique device identifier (UDI) information for a switch and for all the connected devices: the product identification (PID), the version identification (VID), and the serial number
- Message—Record of the hardware-related system messages generated by a switch
- Temperature—Temperature of a switch
- Uptime data—Time when a switch starts, the reason the switch restarts, and the length of time the switch has been running since it last restarted
- Voltage—System voltages of a switch

You should manually set the system clock, or configure it by using Network Time Protocol (NTP). When the switch is running, you can retrieve the OBFL data by using the `show logging onboard` privileged EXEC commands. If the switch fails, contact your Cisco technical support representative to find out how to retrieve the data.

When an OBFL-enabled switch is restarted, there is a 10-minute delay before logging of new data begins.

Configuring OBFL

To enable OBFL, use the `hw-module module logging onboard [message level level]` global configuration command. Use the `message level level` parameter to specify the severity of the hardware-related messages that the switch generates and stores in the flash memory.

To copy the OBFL data to the local network or a specific file system, use the `copy logging onboard module 1 destination` privileged EXEC command.

Caution

We recommend that you keep OBFL enabled and that you do not remove the data stored in the flash memory.
Beginning in privileged EXEC mode, follow these steps to enable and configure OBFL. Note that OBLF is enabled by default; you need to enable it only if it has been disabled.

**Step 1**
```
configure terminal
```
Enter global configuration mode.

**Step 2**
```
hw-module module [slot-number] logging onboard [message level]
```
Enable OBFL on the switch.

You can specify these optional parameters:

- (Optional) `slot-number`—The slot number is always 1 and is not relevant for the switch.
- (Optional) `message level`—Specify the severity level of messages to be generated and stored. The range is from 1 to 7, with 1 being the most severe.

**Step 3**
```
end
```
Return to privileged EXEC mode.

**Step 4**
```
copy logging onboard module [slot-number] destination
```
(Optional) Copy the OBFL data to the local network or a specific file system.

- (Optional) `slot-number`—The slot number is always 1 and is not relevant.
- `destination`—See the `copy logging onboard module` command for destination options.

**Step 5**
```
show logging onboard
```
Verify your entries.

**Step 6**
```
copy running-config startup-config
```
(Optional) Save your entries in the configuration file.

To disable OBFL, use the `no hw-module module 1 logging onboard [message level]` global configuration command.

To clear all the OBFL data in the flash memory except for the uptime and CLI command information, use the `clear logging onboard` privileged EXEC command.

For more information about the commands in this section, see the command reference for this release.

## Displaying OBFL Information

To display the OBFL information, use one or more of the privileged EXEC commands in Table 37-2.

**Note**
When an OBFL-enabled switch is restarted, there is a 10-minute delay before logging of new data begins.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show logging onboard clilog</code></td>
<td>Display the OBFL CLI commands that were entered on a switch.</td>
</tr>
<tr>
<td><code>show logging onboard environment</code></td>
<td>Display the UDI information for a standalone switch and for all the connected FRU devices: the PID, the VID, and the serial number.</td>
</tr>
<tr>
<td><code>show logging onboard message</code></td>
<td>Display the hardware-related messages generated by a switch.</td>
</tr>
</tbody>
</table>
These are examples of output from the show logging onboard commands:

Switch# show logging onboard clillog

CLI LOGGING SUMMARY INFORMATION

COUNT COMMAND

1 hw-module module logging onboard
1 hw-module module logging onboard message level 7
4 show logging onboard
1 show logging onboard message
1 show logging onboard summary

Switch# show logging onboard temp

TEMPERATURE SUMMARY INFORMATION

Number of sensors          : 1
Sampling frequency         : 5 minutes
Maximum time of storage    : 720 minutes

Sensor |   ID  | Maximum Temperature 0C
System | 1     | 41
Temp | Sensor ID
0C  | 1

No historical data to display

Switch# show logging onboard uptime

UPTIME SUMMARY INFORMATION

First customer power on : 03/01/1993 00:06:06
Total uptime            :   0 years  20 weeks   4 days   6 hours  20 minutes
Total downtime          :   0 years   0 weeks   0 days   0 hours   0 minutes
Number of resets        : 90
Number of slot changes  : 0
Current reset reason    : 0x0
Current reset timestamp : 03/01/1993 00:05:43
Current slot            : 1
Current uptime          :   0 years   0 weeks   2 days   6 hours   0 minutes

Reset |        |
Reason | Count |
No historical data to display

Table 37-2 Commands for Displaying OBFL Information (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show logging onboard temperature</td>
<td>Display the temperature of a switch.</td>
</tr>
<tr>
<td>show logging onboard uptime</td>
<td>Display the time when a switch starts, the reason the switch restarts, and the length of time that the switch has been running since it last restarted.</td>
</tr>
<tr>
<td>show logging onboard voltage</td>
<td>Display the system voltages of a switch.</td>
</tr>
</tbody>
</table>
Switch# `show logging onboard voltage`

```
VOLTAGE SUMMARY INFORMATION
Number of sensors : 6
Sampling frequency : 1 minutes
Maximum time of storage : 720 minutes
```

<table>
<thead>
<tr>
<th>Sensor</th>
<th>ID</th>
<th>Maximum Voltage</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.00V</td>
<td>0</td>
<td>12.567</td>
</tr>
<tr>
<td>1.25V</td>
<td>2</td>
<td>1.258</td>
</tr>
<tr>
<td>3.30V</td>
<td>3</td>
<td>3.305</td>
</tr>
<tr>
<td>2.50V</td>
<td>4</td>
<td>2.517</td>
</tr>
<tr>
<td>1.80V</td>
<td>5</td>
<td>1.825</td>
</tr>
<tr>
<td>1.50V</td>
<td>6</td>
<td>1.508</td>
</tr>
</tbody>
</table>

Nominal Range | Sensor ID
--- | ---
No historical data to display

For more information about using the commands in Table 37-2 and for examples of OBFL data, see the command reference for this release.
Configuring Online Diagnostics

This chapter describes how to configure the online diagnostics on the Cisco ME 3800X and ME 3600X switch.

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

- Understanding Online Diagnostics, page 38-1
- Configuring Online Diagnostics, page 38-2
- Running Online Diagnostic Tests, page 38-3

Understanding Online Diagnostics

With online diagnostics, you can test and verify the hardware functionality of the switch while the switch is connected to a live network. The online diagnostics contain packet switching tests that monitor different hardware components and verify the data path and the control signals.

The online diagnostics detect problems in these areas:

- Hardware components
- Interfaces (Ethernet ports and so forth)
- Solder joints

Table 38-1 lists the diagnostic test IDs and names. For information about test attributes, see the output from the `show diagnostic content` privileged EXEC command.

<table>
<thead>
<tr>
<th>Test ID Number</th>
<th>Test Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TestPortAsicMem [B<em>D</em>R**]</td>
</tr>
<tr>
<td>2</td>
<td>TestPortAsicCam [B<em>D</em>R**]</td>
</tr>
<tr>
<td>3</td>
<td>TestPortAsicLoopback[B<em>D</em>R**]</td>
</tr>
<tr>
<td>4</td>
<td>TestPortLoopback [B<em>D</em>R**]</td>
</tr>
<tr>
<td>5</td>
<td>TestFpga [B<em>D</em>R**]</td>
</tr>
</tbody>
</table>
Online diagnostics are categorized as on-demand, scheduled, or health-monitoring diagnostics.

- On-demand diagnostics run from the CLI.
- Scheduled diagnostics run at user-designated intervals or at specified times when the switch is connected to a live network.

## Configuring Online Diagnostics

You must configure the failure threshold and the interval between tests before enabling diagnostic monitoring. You can schedule online diagnostics to run at a designated time of day or on a daily, weekly, or monthly basis. Use the no form of this command to remove the scheduling. For detailed information about this command, see the command reference for this release.

Beginning in privileged EXEC mode, follow these steps to schedule online diagnostics:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
</tr>
</tbody>
</table>
| Step 2  | `diagnostic schedule test {name | test-id | test-id-range | all | basic} {daily hh:mm | on mm dd yyyy hh:mm | weekly day-of-week hh:mm}` | Schedule on-demand diagnostic tests for a specific day and time. When specifying the tests to be scheduled, use these options:  
  - name—Name of the test that appears in the `show diagnostic content` command output. See Table 38-1.  
  - test-id—ID number of the test that appears in the `show diagnostic content` command output. See Table 38-1.  
  - test-id-range—A range of test ID numbers separated by a hyphen or commas.  
  - all—All of the diagnostic tests.  
  - basic—Basic on-demand diagnostic tests.  
You can schedule the tests for these time periods:  
  - Daily—Use the `daily hh:mm` parameter.  
  - Specific day and time—Use the `on mm dd yyyy hh:mm` parameter.  
  - Weekly—Use the `weekly day-of-week hh:mm` parameter. |
| Step 3  | `show diagnostic {content | schedule}` | Verify the configured online diagnostic tests and schedule.  
  - Enter `show diagnostic content` to display the configured online diagnostics.  
  - Enter `show diagnostic schedule` to display the online diagnostics test schedule. |
| Step 4  | `copy running-config startup-config` | (Optional) Save your entries in the configuration file. |

Use the `no diagnostic schedule test {name | test-id | test-id-range | all | basic} {daily hh:mm | on mm dd yyyy hh:mm | weekly day-of-week hh:mm}` global configuration command to remove the scheduled tests.

This example shows how to schedule diagnostic testing for a specific day and time and verify the schedule:

```
Switch(config)# diagnostic schedule test 1 on Dec 4 2008 10:22
```
Switch(config)# end
Switch# show diagnostic schedule
Current Time = 10:21:24 UTC Thu Dec 4 2008

Diagnostic:

Schedule #1:
   To be run on December 4 2008 10:22
   Test ID(s) to be executed: 1.

At the scheduled time, the switch runs the test:

Switch# 
Dec 4 10:21:59.492: %DIAG-6-SCHED_RUNNING: : Performing Scheduled Online Diagnostic...
Dec 4 10:21:59.492: %DIAG-6-TEST_RUNNING: : Running TestPortAsicStackPortLoopback(ID=1) ..
Dec 4 10:22:00.498: %DIAG-6-TEST_OK: : TestPortAsicStackPortLoopback(ID=1) has completed successfully
Dec 4 10:22:00.498: %DIAG-6-SCHED_COMPLETE: : Scheduled Online Diagnostic is completed

For more examples, see the “Examples” section for the `diagnostic schedule` command in the command reference for this release.

**Running Online Diagnostic Tests**

After you configure online diagnostics, you can manually start diagnostic tests or display the test results. You can also see the tests configured for the switch and the tests that have already run.

- Starting Online Diagnostic Tests, page 38-3
- Displaying Online Diagnostic Tests and Results, page 38-4

**Starting Online Diagnostic Tests**

After you configure diagnostic tests to run on the switch, use the `diagnostic start` privileged EXEC command to begin diagnostic testing.

---

**Note**

After starting the tests, you cannot stop the testing process.
### Running Online Diagnostic Tests

This example shows how to start a diagnostic test by using the test name:

```
Switch# diagnostic start test TestPortAsicRingLoopback
```

This example shows how to start all of the basic diagnostic tests:

```
Switch# diagnostic start test all
```

### Displaying Online Diagnostic Tests and Results

You can display the configured online diagnostic tests and review the test results by using the privileged EXEC `show` commands in Table 38-2.

#### Table 38-2 Commands for Diagnostic Test Configuration and Results

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show diagnostic content</td>
<td>Displays the online diagnostics configured for a switch.</td>
</tr>
<tr>
<td>show diagnostic status</td>
<td>Displays the running diagnostic tests.</td>
</tr>
<tr>
<td>show diagnostic result [detail</td>
<td>test {name</td>
</tr>
<tr>
<td>show diagnostic switch [detail]</td>
<td></td>
</tr>
<tr>
<td>show diagnostic schedule</td>
<td>Displays the online diagnostics test schedule.</td>
</tr>
<tr>
<td>show diagnostic post</td>
<td>Displays the POST results. (The output is the same as the <code>show post</code> command output.)</td>
</tr>
</tbody>
</table>

This is an example of the output from the `show diagnostic result` command:

```
Switch# show diagnostic result

: SerialNo : FOC1225U4CY

Overall diagnostic result: PASS

Test results: (. = Pass, F = Fail, U = Untested)
```
1) TestPortAsicStackPortLoopback ---> .
2) TestPortAsicLoopback ------------> U
3) TestPortAsicCam -----------------> U
4) TestPortAsicRingLoopback --------> U
5) TestMicRingLoopback --------------> U
6) TestPortAsicMem ------------------> U

This is an example of the output from the `show diagnostic post` command:

```
Switch# show diagnostic post
Stored system POST messages:

Switch 1
--------

POST: CPU MIC register Tests : Begin
POST: CPU MIC register Tests : End, Status Passed

POST: PortASIC Memory Tests : Begin
POST: PortASIC Memory Tests : End, Status Passed

POST: CPU MIC interface Loopback Tests : Begin
POST: CPU MIC interface Loopback Tests : End, Status Passed

POST: PortASIC RingLoopback Tests : Begin
POST: PortASIC RingLoopback Tests : End, Status Passed

POST: Thermal, Fan Tests : Begin
POST: Thermal, Fan Tests : End, Status Passed

POST: PortASIC CAM Subsystem Tests : Begin
POST: PortASIC CAM Subsystem Tests : End, Status Passed

POST: PortASIC Port Loopback Tests : Begin
POST: PortASIC Port Loopback Tests : End, Status Passed

POST: EMAC Loopback Tests : Begin
POST: EMAC Loopback Tests : End, Status Passed
```

For more examples of other `show diagnostic` command outputs, see the “Examples” section of the `show diagnostic` command in the command reference for this release.
Supported MIBs

This appendix lists the supported management information base (MIBs) for this release on the Cisco ME 3800X and ME 3600X switch.

TDR MIB also supported

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

MIB List

- BGP4-MIB
- BRIDGE-MIB

Note: 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.

- CISCO-CDP-MIB
- CISCO-CLASS-BASED-QOS-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENTITY-SENSOR MIB
- CISCO-ETHER-CFM-MIB
- CISCO-FLASH-MIB
- CISCO-HSRP-MIB
- CISCO-IETF-PW-MIB
- CISCO-IMAGE-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-NAC-NAD-MIB
- CISCO-PAE-MIB
- CISCO-PAGP-MIB
- CISCO-PROCESS-MIB
- CISCO-RESILIENT-ETHERNET-PROTOCOL-MIB
- CISCO-STP-EXTENSIONS-MIB
- CISCO-VTP-MIB
- DOM MIB
- ENTITY-MIB
- HOST-RESOURCES-MIB
- IF-MIB
- IF-Table
- IS-IS MIB
- LLDP MIB
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-SYS-MIB
- OSPF-MIB
- RFC1213-MIB (Functionality is as per the agent capabilities specified in the CISCO-RFC1213-CAPABILITY.my.)
- RMON-MIB
- RMON2-MIB
- SNMPv2-MIB
- TDR-MIB

**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 obtain 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.
Using FTP to Access the MIB Files
APPENDIX B

Working with the Cisco IOS File System, Configuration Files, and Software Images

This appendix describes how to manipulate the Cisco ME 3800X and ME 3600X 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*.

- Working with the Flash File System, page B-1
- Working with Configuration Files, page B-8
- Working with Software Images, page B-23

## 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:`.

- 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-6
- Displaying the Contents of a File, page B-8
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 nvram rw nvram:
      -           -  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><code>flash</code>—The file system is for a flash memory device.</td>
</tr>
<tr>
<td></td>
<td><code>nvram</code>—The file system is for a NVRAM device.</td>
</tr>
<tr>
<td></td>
<td><code>opaque</code>—The file system is a locally generated pseudo file system (for example, the <code>system</code>) or a download interface, such as brimux.</td>
</tr>
<tr>
<td></td>
<td><code>unknown</code>—The file system is an unknown type.</td>
</tr>
<tr>
<td>Flags</td>
<td>Permission for file system.</td>
</tr>
<tr>
<td></td>
<td><code>ro</code>—read-only.</td>
</tr>
<tr>
<td></td>
<td><code>rw</code>—read/write.</td>
</tr>
<tr>
<td></td>
<td><code>wo</code>—write-only.</td>
</tr>
<tr>
<td>Prefixes</td>
<td>Alias for file system.</td>
</tr>
<tr>
<td></td>
<td><code>flash:</code>—Flash file system.</td>
</tr>
<tr>
<td></td>
<td><code>nvram:</code>—NVRAM.</td>
</tr>
<tr>
<td></td>
<td><code>null:</code>—Null destination for copies. You can copy a remote file to null to find its size.</td>
</tr>
<tr>
<td></td>
<td><code>system:</code>—Contains the system memory, including the running configuration.</td>
</tr>
<tr>
<td></td>
<td><code>tftp:</code>—TFTP network server.</td>
</tr>
<tr>
<td></td>
<td><code>xmodem:</code>—Obtain the file from a network machine by using the Xmodem protocol.</td>
</tr>
<tr>
<td></td>
<td><code>ymodem:</code>—Obtain the file from a network machine by using the Ymodem protocol.</td>
</tr>
</tbody>
</table>
Appendix B  Working with the Cisco IOS File System, Configuration Files, and Software Images

Working with the Flash File System

Setting the Default File System

You can specify the file system or directory that the system uses as the default file system by using the `cd filesystem:` privileged EXEC command. You can set the default file system to omit the `filesystem:` argument from related commands. For example, for all privileged EXEC commands that have the optional `filesystem:` argument, the system uses the file system specified by the `cd` command.

By default, the default file system is `flash:`.

You can display the current default file system as specified by the `cd` command by using the `pwd` privileged EXEC command.

Displaying Information about Files on a File System

You can view a list of the contents of a file system before manipulating its contents. For example, before copying a new configuration file to flash memory, you might want to verify that the file system does not already contain a configuration file with the same name. Similarly, before copying a flash configuration file to another location, you might want to verify its filename for use in another command.

To display information about files on a file system, use one of the privileged EXEC commands in Table 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>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>dir filesystem:</code></td>
<td>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>2</td>
<td><code>cd new_configs</code></td>
<td>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>3</td>
<td><code>pwd</code></td>
<td>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><strong>dir filesystem:</strong> Display the directories on the specified file system.</td>
</tr>
<tr>
<td></td>
<td>For <strong>filesystem:</strong> use <strong>flash:</strong> for the system board flash device.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>mkdir old_configs</strong> Create a new directory.</td>
</tr>
<tr>
<td></td>
<td>The command example shows how to create the directory named <strong>old_configs</strong>.</td>
</tr>
<tr>
<td></td>
<td>Directory names are case sensitive.</td>
</tr>
<tr>
<td></td>
<td>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><strong>dir filesystem:</strong> 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`
In addition, the Secure Copy Protocol (SCP) 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. See the “Configuring the Switch for Secure Copy Protocol” section on page 9-39.


Local writable file systems include flash:

Some invalid combinations of source and destination exist. Specifically, you cannot copy these combinations:

- From a running configuration to a running configuration
- From a startup configuration to a startup configuration
- From a device to the same device (for example, the `copy flash: flash:` command is invalid)

For specific examples of using the `copy` command with configuration files, see the “Working with Configuration Files” section on page B-8.

To copy software images either by downloading a new version or by uploading the existing one, use the `archive download-sw` or the `archive upload-sw` privileged EXEC command. For more information, see the “Working with Software Images” section on page B-23.

### 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.

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:

\[ \text{archive tar /create destination-url flash:/file-url} \]

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://[[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:

\[ \text{archive tar /table source-url} \]

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-file.tar
```

For the TFTP, the syntax is
```
tftp://[location]/directory]/tar-file.tar
```

The `tar-file.tar` is the tar file to display.

This example shows how to display the contents of a switch tar file that is in flash memory:

Switch# `archive tar /table flash:image-name.tar`
```
info (219 bytes)
image-name/ (directory)
image-name/html/ (directory)
image-name/html/foo.html (0 bytes)
image-name/image-name.bin (4527884 bytes)
image-name/info (346 bytes)
info (110 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/@location]/directory]/tar-file.tar`

- For the RCP, the syntax is
  `rcp://[username@location]/directory]/tar-file.tar`

- For the TFTP, the syntax is
  `tftp://[location]/directory]/tar-file.tar`

The `tar-file.tar` is the tar file from which to extract files.

For `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`
Appendix B      Working with the Cisco IOS File System, Configuration Files, and Software Images

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 | ebcidic] 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.

These sections contain this configuration information:

- Guidelines for Creating and Using Configuration Files, page B-9
- Configuration File Types and Location, page B-9
- Creating a Configuration File By Using a Text Editor, page B-10
- Copying Configuration Files By Using TFTP, page B-10
- Copying Configuration Files By Using FTP, page B-12
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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>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-11, the “Downloading a Configuration File By Using FTP” section on page B-13, or the “Downloading a Configuration File By Using RCP” section on page B-17.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Open the configuration file in a text editor, such as vi or emacs on UNIX or Notepad on a PC.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Extract the portion of the configuration file with the desired commands, and save it in a new file.</td>
</tr>
<tr>
<td>Step 4</td>
<td>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).</td>
</tr>
<tr>
<td>Step 5</td>
<td>Make sure the permissions on the file are set to world-read.</td>
</tr>
</tbody>
</table>

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.

These sections contain this configuration information:

- Preparing to Download or Upload a Configuration File By Using TFTP, page B-10
- Downloading the Configuration File By Using TFTP, page B-11
- 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:
  
  tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
  
  Make sure that the /etc/services file contains this line:
  
  tftp 69/udp
  
  **Note** You must restart the inetd daemon after modifying the /etc/inetd.conf and /etc/services files. To restart the daemon, either stop the inetd process and restart it, or enter a fastboot command (on the SunOS 4.x) or a reboot command (on Solaris 2.x or SunOS 5.x). For more information on the TFTP daemon, 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-read.

• Before uploading the configuration file, you might need to create an empty file on the TFTP server. To create an empty file, enter the touch filename command, where filename is the name of the file you will use when uploading it to the server.

• During upload operations, if you are overwriting an existing file (including an empty file, if you had to create one) on the server, ensure that the permissions on the file are set correctly. Permissions on the file should be world-write.

### Downloading the Configuration File By Using TFTP

To configure the 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.

---

This example shows how to configure the software from the file `tokyo-confg` at IP address 172.16.2.155:

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

### Uploading the Configuration File By Using TFTP

To upload a configuration file from a switch to a TFTP server for storage, follow these steps:

---

**Step 1** Verify that the TFTP server is properly configured by referring to the “Preparing to Download or Upload a Configuration File By Using TFTP” section on page B-10.

**Step 2** Log into the switch through the console port or a Telnet session.

**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.

These sections contain this configuration information:

- Preparing to Download or Upload a Configuration File By Using FTP, page B-13
- Downloading a Configuration File By Using FTP, page B-13
- Uploading a Configuration File By Using FTP, page B-14
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 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

Starting 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-13.</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 on the switch.</td>
</tr>
<tr>
<td><strong>configure terminal</strong></td>
<td>This step is required only if you override the default remote username or password (see Steps 4, 5, and 6).</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) Change the default remote username.</td>
</tr>
<tr>
<td><strong>ip ftp username username</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) Change the default password.</td>
</tr>
<tr>
<td><strong>ip ftp password password</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>end</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></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><strong>copy</strong>ftp://username[:password]@location/directory/filename** system:running-config</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td><strong>copy</strong>ftp://username[:password]@location/directory/filename** nvram:startup-config</td>
<td></td>
</tr>
</tbody>
</table>
This example shows how to copy a configuration file named `host1-config` from the `netadmin1` directory on the remote server with an IP address of 172.16.101.101 and to load and run those commands on the switch:

```
Switch# copy ftp://netadmin1:mypass@172.16.101.101/host1-config system:running-config
Configure using host1-config from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-config:[OK]
Switch#
%SYS-5-CONFIG: Configured from host1-config by ftp from 172.16.101.101
```

This example shows how to specify a remote username of `netadmin1`. The software copies the configuration file `host2-config` from the `netadmin1` directory on the remote server with an IP address of 172.16.101.101 to the 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-config]? host2-config
Configure using host2-config from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-config:[OK]
%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>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 verify ftp server</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-13.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Log into the switch through the console port or a Telnet session.</td>
</tr>
<tr>
<td>Step 3 ip ftp username username</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 password password</td>
<td>(Optional) Change the default remote username.</td>
</tr>
<tr>
<td>Step 5</td>
<td>(Optional) Change the default password.</td>
</tr>
</tbody>
</table>
Appendix B  Working with the Cisco IOS File System, Configuration Files, and Software Images

Working with Configuration Files

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 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:

```
Switch# configure terminal
Switch(config)# ip ftp username netadmin2
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# copy nvram:startup-config ftp://netadmin1: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]
```

Copying 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-user name username` global configuration command if the command is configured.
Appendix B   Working with the Cisco IOS File System, Configuration Files, and Software Images

Working with Configuration Files

- 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.

These sections contain this configuration information:

- Preparing to Download or Upload a Configuration File By Using RCP, page B-16
- Downloading a Configuration File By Using RCP, page B-17
- Uploading a Configuration File By Using RCP, page B-18

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.
Working with Configuration Files

Appendix B      Working with the Cisco IOS File System, Configuration Files, and Software Images

Download 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>Step 1</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-16.</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>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>(Optional) Specify the remote username.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6</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-config from the netadmin1 directory on the remote server with an IP address of 172.16.101.101 and load and run those commands on the switch:

```
Switch# copy rcp://netadmin1@172.16.101.101/host1-config system:running-config
Configure using host1-config from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-config:![OK]
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-config 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://netadmin1@172.16.101.101/host2-config nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-config]? host2-config
Configure using host2-config from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-config:![OK]
[OK]
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>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 a Configuration File By Using RCP” section on page B-16.</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>Step 4</td>
<td>ip rcmd remote-username username</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy system:running-config rcp://username@location/directory/filename</td>
</tr>
<tr>
<td>or</td>
<td>copy nvram:startup-config rcp://username@location/directory/filename</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-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:

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin2
Switch(config)# end
Switch# copy nvram:startup-config rcp://netadmin2@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]
```

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-19
- Configuration Replacement and Rollback Guidelines, page B-20
- Configuring the Configuration Archive, page B-21
- Performing a Configuration Replacement or Rollback Operation, page B-22

Understanding Configuration Replacement and Rollback

- Archiving a Configuration, page B-19
- Replacing a Configuration, page B-20
- Rolling Back a Configuration, page B-20

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.
Appendix B      Working with the Cisco IOS File System, Configuration Files, and Software Images

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 target-url` privileged EXEC 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 Replacement and Rollback Guidelines**

- 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>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>archive</td>
<td>Enter archive configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>path <code>url</code></td>
<td>Specify the location and filename prefix for the files in the configuration archive.</td>
</tr>
<tr>
<td>Step 4</td>
<td>maximum <code>number</code></td>
<td>(Optional) Set the maximum number of archive files of the running configuration to be saved in the configuration archive. <code>number</code>—Maximum files of the running configuration file in the configuration archive. Valid values are from 1 to 14. The default is 10. <strong>Note</strong> Before using this command, you must first enter the <code>path archive configuration</code> command to specify the location and filename prefix for the files in the configuration archive.</td>
</tr>
<tr>
<td>Step 5</td>
<td>time-period <code>minutes</code></td>
<td>(Optional) Set the time increment for automatically saving an archive file of the running configuration in the configuration archive. <code>minutes</code>—Specify how often, in minutes, to automatically save an archive file of the running configuration in the configuration archive.</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 the configuration.</td>
</tr>
<tr>
<td>Step 8</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Performing a Configuration Replacement or Rollback Operation

Beginning in privileged EXEC mode, follow these steps to replace the running configuration file with a saved configuration file:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>archive config</td>
<td>(Optional) Save the running configuration file to the configuration archive. <strong>Note</strong> Enter the <code>path</code> archive configuration command before using this command.</td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>configure terminal</td>
<td>Make necessary changes to the running configuration.</td>
</tr>
<tr>
<td>4</td>
<td>exit</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>5</td>
<td>configure replace <code>target-url</code> [list] [force] [time <code>seconds</code>] [nolock]</td>
<td>Replace the running configuration file with a saved configuration file. <code>target-url</code>—URL (accessible by the file system) of the saved configuration file that is to replace the running configuration, such as the configuration file created in Step 2 by using the <code>archive config</code> privileged EXEC command. <code>list</code>—Display a list of the command entries applied by the software parser during each pass of the configuration replacement operation. The total number of passes also appears. <code>force</code>—Replace the running configuration file with the specified saved configuration file without prompting you for confirmation. <code>time </code>seconds<code>—Specify the time (in seconds) within which you must enter the </code>configure confirm<code>command to confirm replacement of the running configuration file. If you do not enter the</code>configure confirm<code>command within the specified time limit, the configuration replacement operation is automatically stopped. (In other words, the running configuration file is restored to the configuration that existed before you entered the</code>configure replace<code>command). **Note** You must first enable the configuration archive before you can use the</code>time <code>seconds</code> command line option. <code>nolock</code>—Disable the locking of the running configuration file that prevents other users from changing the running configuration during a configuration replacement operation.</td>
</tr>
<tr>
<td>6</td>
<td>configure confirm</td>
<td>(Optional) Confirm replacement of the running configuration with a saved configuration file. <strong>Note</strong> Use this command only if the <code>time </code>seconds<code>keyword and argument of the</code>configure replace` command are specified.</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>
Working with Software Images

This section describes how to archive (download and upload) software image files, which contain the system software, the Cisco IOS code, and the embedded device manager software.

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 can download a switch image file from a TFTP, FTP, or RCP server to upgrade the switch software. For information about upgrading your switch by using a TFTP server, see the release notes.

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 to another of the same type.

The protocol that 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.

These sections contain this configuration information:

- Image Location on the Switch, page B-23
- tar File Format of Images on a Server or Cisco.com, page B-24
- Copying Image Files By Using TFTP, page B-27
- Copying Image Files By Using FTP, page B-27
- Copying Image Files By Using RCP, page B-32

For a list of software images and the supported upgrade paths, see the release notes for 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. A subdirectory contains the files needed for web management. The image is stored on the system board flash memory (flash:).

You can use the `show version` privileged EXEC command to see the software version that is currently running on your 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 that you might have stored in flash memory.
tar File Format of Images on a Server or Cisco.com

Software images located on a server or downloaded from Cisco.com are provided in a tar file format, which contains these files:

- 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: universal-122-52.0.112.EY
version_directory: me380x-universal.mz.122-52.111.EY
image_system_type_id: 0x00000000
image_name: me380x-universal.mz.122-52.111.EY.bin
ios_image_file_size: 16527872
total_image_file_size: 20685312
image_feature: IP|LAYER_2|MIN_DRAM_MEG=128
image_family: ME380x
board_ids: 0x00000029
info_end:
```

<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 and the HTML subdirectory are 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 and the web management 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.

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.
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:

  ```
  tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
  ```

  Make sure that the `/etc/services` file contains this line:

  ```
  tftp 69/udp
  ```

  **Note** You must restart the inetd daemon after modifying the `/etc/inetd.conf` and `/etc/services` files. To restart the daemon, either stop the inetd process and restart it, or enter a `fastboot` command (on the SunOS 4.x) or a `reboot` command (on Solaris 2.x or SunOS 5.x). For more information on the TFTP daemon, 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, perform Steps 1 and 2 and Step 4.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>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-25.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Log into the switch through the console port or a Telnet session.</td>
</tr>
</tbody>
</table>
| **Step 3** | 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** | 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.
If you specify the */leave-old-sw*, the existing files are not removed. If there is not enough space to install the new image and keep the current running image, the download process stops, and an error message is displayed.

The algorithm installs the downloaded image on the system board flash device (flash:). The image is placed into a new directory named with the software version string, and the 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 &quot;Preparing to Download or Upload an Image File By Using TFTP&quot; section on page B-25.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Log into the switch through the console port or a Telnet session.</td>
</tr>
</tbody>
</table>
| Step 3  | Upload the currently running switch image to the TFTP server.  
archive upload-sw tftp://location/directory/image-name.tar  
- For //location, specify the IP address of the TFTP server.  
- For /directory/image-name.tar, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. The image-name.tar is the name of the software image to be stored on the server. |

The archive upload-sw privileged EXEC command builds an image file on the server by uploading these files in order: info, the Cisco IOS image, and the web management files. 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.

**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.

These sections contain this configuration information:

- Preparing to Download or Upload an Image File By Using FTP, page B-28
- Downloading an Image File By Using FTP, page B-29
- Uploading an Image File By Using FTP, page B-31

### Preparing to Download or Upload an Image File By Using FTP

You can copy images files to or from an FTP server.

The FTP protocol requires a client to send a remote username and password on each FTP request to a server. When you copy an image file from the 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, perform Steps 1 through 6 and skip to Step 8.

<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 an Image File By Using FTP” section on page B-28.</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><code>configure terminal</code></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 or password (see Steps 4, 5, and 6).</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>ip ftp username username</code></td>
</tr>
<tr>
<td></td>
<td>(Optional) Change the default remote username.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>ip ftp password password</code></td>
</tr>
<tr>
<td></td>
<td>(Optional) Change the default password.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td></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.

- If the flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the `/overwrite` option.

- If you specify the `/leave-old-sw`, the existing files are not removed. If there is not enough space to install the new image and keep the running image, the download process stops, and an error message is displayed.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
<td>Download the image file from the FTP server to the switch, and overwrite the current image.</td>
</tr>
<tr>
<td><code>archive download-sw /overwrite /reload</code></td>
<td>- The <code>/overwrite</code> option overwrites the software image in flash memory with the downloaded image.</td>
</tr>
<tr>
<td><code>ftp:[[//username[::password@location]/directory]//image-name.tar</code></td>
<td>- The <code>/reload</code> option reloads the system after downloading the image unless the configuration has been changed and not been saved.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Download the image file from the FTP server to the switch, and keep the current image.</td>
</tr>
<tr>
<td><code>archive download-sw /leave-old-sw /reload</code></td>
<td>- The <code>/leave-old-sw</code> option keeps the old software version after a download.</td>
</tr>
<tr>
<td><code>ftp:[[//username[::password@location]/directory]//image-name.tar</code></td>
<td>- The <code>/reload</code> option reloads the system after downloading the image unless the configuration has been changed and not been saved.</td>
</tr>
</tbody>
</table>

Note: 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-28.

Note: For `@location`, specify the IP address of the FTP server.

Note: For `directory//image-name.tar`, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

---

Step 7:

```
archive download-sw /overwrite /reload
ftp:[[//username[::password@location]/directory]//image-name.tar
```

Step 8:

```
archive download-sw /leave-old-sw /reload
ftp:[[//username[::password@location]/directory]//image-name.tar
```
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.

Use the upload feature only if the web management pages associated with the embedded device manager have been installed with the existing image.

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><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-13.</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><code>configure terminal</code> 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><strong>Step 4</strong></td>
<td><code>ip ftp username username</code> (Optional) Change the default remote username.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>ip ftp password password</code> (Optional) Change the default password.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
| **Step 7** | `archive upload-sw ftp:[][//username[:password]@][location][directory]/image-name.tar` Upload the currently running switch image to the FTP server.  
  • For `username:password`, specify the username and password. These must be associated with an account on the FTP server. For more information, see the “Preparing to Download or Upload an Image File By Using FTP” section on page B-28.  
  • For `@location`, specify the IP address of the FTP server.  
  • For `directory/image-name.tar`, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. The `image-name.tar` is the name of the software image to be stored on the server. |
The **archive upload-sw** command builds an image file on the server by uploading these files in order: info, the Cisco IOS image, and the web management files. 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 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.

These sections contain this configuration information:

- Preparing to Download or Upload an Image File By Using RCP, page B-32
- Downloading an Image File By Using RCP, page B-33
- Uploading an Image File By Using RCP, page B-35

### 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 User Datagram Protocol (UDP), a connectionless protocol, RCP uses TCP, which is connection-oriented.

To use RCP to copy files, the server from or to which you will be copying files must support RCP. The RCP copy commands rely on the rsh server (or daemon) on the remote system. To copy files by using RCP, you do not need to create a server for file distribution as you do with TFTP. You only need to have access to a server that supports the remote shell (rsh). (Most UNIX systems support rsh.) Because you are copying a file from one place to another, you must have read permission on the source file and write permission on the destination file. If the destination file does not exist, RCP creates it for you.

RCP requires a client to send a remote username on each RCP request to a server. When you copy an image from the 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, perform Steps 1 through 5 and go to Step 7.

<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 an Image File By Using RCP” section on page B-32.</td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------</td>
<td>---------</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>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><strong>Step 4</strong></td>
<td><code>ip rcmd remote-username username</code> (Optional) Specify the remote username.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
| **Step 6** | `archive download-sw /overwrite /reload rcp:[][//username@]location]/directory]/image-name.tar]` Download the image file from the RCP 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`, 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-32.  
- 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. |
| **Step 7** | `archive download-sw /leave-old-sw /reload rcp:[][//username@]location]/directory]/image-name.tar]` Download the image file from the RCP server to the 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`, 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-32.  
- 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 an keep the running image, the download process stops, and an error message is displayed.

The algorithm installs the downloaded image onto the system board flash device (`flash:`). The image is placed into a new directory named with the software version string, and the BOOT environment variable is updated to point to the newly installed image.

If you kept the old software during the download process (you specified the `/leave-old-sw` keyword), you can remove it by entering the `delete /force /recursive filesystem:/file-url` privileged EXEC command. For `filesystem`, use `flash:` for the system board flash device. For `file-url`, enter the directory name of the old software image. All the files in the directory and the directory are removed.

**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.

The upload feature should be used only if the web management pages associated with the embedded device manager have been installed with the existing image.

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><strong>Step 1</strong></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-32.</td>
</tr>
<tr>
<td>Step 2</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. This step is required only if you override the default remote username (see Steps 4 and 5).</td>
</tr>
<tr>
<td><code>ip rcmd remote-username username</code></td>
<td>(Optional) Specify the remote username.</td>
</tr>
</tbody>
</table>
Step 5

end

Return to privileged EXEC mode.

Step 6

archive upload-sw
rcp:[]//[]username@[]location[]directory[]image-name.tar]

Upload the currently running switch image to the RCP server.

- For //username, specify the username; for the RCP copy request to execute, an account must be defined on the network server for the remote username. For more information, see the “Preparing to Download or Upload an Image File By Using RCP” section on page B-32.
- For @location, specify the IP address of the RCP server.
- For /directory/image-name.tar, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive.
- The image-name.tar is the name of software image to be stored on the server.

The archive upload-sw privileged EXEC command builds an image file on the server by uploading these files in order: info, the Cisco IOS image, and the web management files. 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 15.1(2)EY

This appendix lists some of the command-line interface (CLI) commands that appear when you enter the question mark (?) at the Cisco Metro Ethernet (ME) 3800X and ME 3600X switch prompt but are not supported in this release, either because they are not tested or because of switch hardware limitations. This is not a complete list. The unsupported commands are listed by software feature and command mode or they are listed by command mode under “Other Unsupported Commands.”

- Access Control List Commands, page C-2
- Address Resolution Protocol (ARP) Commands, page C-2
- IGMP Snooping Commands, page C-3
- IP Multicast Routing Commands, page C-3
- IP Network Address Translation (NAT) Commands, page C-4
- IP Unicast Routing Commands, page C-4
- Multiprotocol Label Switching (MPLS) Commands, page C-6
- Multicast Source Discovery Protocol (MSDP) Commands, page C-7
- NetFlow Commands, page C-8
- Quality of Service (QoS) Commands, page C-8
- RADIUS Commands, page C-8
- Simple Network Management Protocol (SNMP) Commands, page C-9
- Spanning Tree Commands, page C-9
- VLAN Commands, page C-9
- Other Unsupported Commands, page C-10
Access Control List Commands

Privileged EXEC Mode

access-enable [host] [timeout minutes]
access-template
clear access-template
show arp access-list

Global Configuration Mode

arp access-list
access-list rate-limit acl-index {precedence | mask prec-mask}
access-list dynamic extended

Address Resolution Protocol (ARP) Commands

Global Configuration Mode

arp ip-address hardware-address smds
arp ip-address hardware-address srp-a
arp ip-address hardware-address srp-b

Interface Configuration Mode

arp probe

Hot Standby Routing Protocol (HSRP) Commands

Global Configuration Mode

interface Async
interface BVI
interface Dialer
interface Group-Async
interface Lex
interface Virtual-Template
interface Virtual-Tokenring
IGMP Snooping Commands

Global Configuration Mode

   ip igmp snooping source-only-learning

IP Multicast Routing Commands

Privileged EXEC Mode

   clear ip dvmrp route commands
   debug ip dvmrp commands
   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.
   debug ip pim atm
   show ip dvmrp route commands
   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.

Global Configuration Mode

   All ip dvmrp commands
   ip multicast-routing vrf vrf-name
   ip pim accept-rp
   ip pim register-rate-limit

Interface Configuration Mode

   All ip dvmrp commands
   ip igmp helper-address ip-address
IP Network Address Translation (NAT) Commands

Privileged EXEC Mode

- show ip nat portblock
- show ip nat statistics
- show ip nat translations

Global Configuration Mode

- ip nat create
- ip nat inside
- ip nat log
- ip nat service
- ip nat translation

Interface Configuration Mode

- ip nat inside
- ip nat outside

IP Unicast Routing Commands

Privileged EXEC or User EXEC Mode

- clear ip accounting [checkpoint]
- clear ip bgp address flap-statistics
- show cef [drop | not-cef-switched]
- show ip accounting [checkpoint] [output-packets | access-violations]
- show ip bgp dampened-paths

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 pim nbma-mode
show ip bgp inconsistent-as
show ip bgp regexp regular expression
show ipv6 (all)

Global Configuration Mode

ip accounting-list ip-address wildcard
ip accounting-transits count
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
router iso-igrp
router mobile
router odr

Interface Configuration Mode

dampening
ip accounting
ip load-sharing [per-packet]
ip mtu bytes
ip ospf dead-interval minimal hello-multiplier multiplier
ip unnumbered type number
All ip security commands

BGP Router Configuration Mode

default-information originate
neighbor advertise-map
neighbor allowas-in
neighbor default-originate
neighbor description
network backdoor
table-map
Appendix C  Unsupported Commands in Cisco IOS Release 15.1(2)EY

Route Map Configuration Mode

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 precedence value
set ip qos-group
set metric-type internal
set origin
set metric-type internal

VPN Configuration Mode

All

Multiprotocol Label Switching (MPLS) Commands

Privileged EXEC or User EXEC Mode

dereg debug ip rsvp hello [bfd | detail | stats]
dereg debug ip rsvp sso
dereg debug mpls traffic-eng exp
dereg debug mpls traffic-eng forwarding-adjacency
dereg debug mpls traffic-eng ha
dereg show ip rsvp fast-reroute
dereg show ip rsvp hello [instance | statistics]
dereg show mpls traffic-eng exp
dereg show mpls traffic-eng forwarding-adjacency

Global Configuration Mode

ip rsvp signalling hello [bfd | graceful-restart]
mlps traffic-eng auto-bw
mlps traffic-eng lsp
Interface Configuration Mode

Physical Interfaces

ip rsvp bandwidth {mam | rdm}
ip rsvp signalling hello [bfd | dscp | fast-reroute | graceful-restart | refresh | reroute]
mls 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

Routing Configuration Mode

interface auto-template
mls traffic-eng mesh-group (ISIS mode)
mls traffic-eng multicast-intact (ISIS mode and OSPF mode)
tunnel destination mesh-group

Multicast Source Discovery Protocol (MSDP) Commands

Privileged EXEC Mode

show access-expression
show exception
show pm LINE
show smf [interface-id]
show subscriber-policy [policy-number]
show template [template-name]
Global Configuration Mode

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.)

NetFlow Commands

Global Configuration Mode

ip flow-aggregation cache
ip flow-cache entries

Quality of Service (QoS) Commands

Global Configuration Mode

priority-list

Interface Configuration Mode

priority-group

RADIUS Commands

Global Configuration Mode

aaa authentication feature default enable
aaa authentication feature default line
aaa nas port extended
authentication command bounce-port ignore
authentication command disable-port ignore
radius-server attribute nas-port
radius-server configure
radius-server extended-portnames
Simple Network Management Protocol (SNMP) Commands

Global Configuration Mode

- snmp-server enable informs
- snmp-server ifindex persist

Spanning Tree Commands

Global Configuration Mode

- spanning-tree pathcost method {long | short}
- spanning-tree transmit hold-count

Interface Configuration Mode

- spanning-tree stack-port

VLAN Commands

Global Configuration Mode

- vlan internal allocation policy {ascending | descending}

Global Configuration Mode

- vlan internal allocation policy {ascending | descending}

VLAN Configuration Mode

- remote-span
Other Unsupported Commands

Privileged EXEC and User EXEC Mode

All event manager commands
renew ip dhcp snooping database
test cable-diagnostics prbs
verify

Clear Commands

All clear dot1x commands
clear ip arp inspection
All clear ip dhcp snooping commands
All clear ipv6 commands

Debug Commands

All debug dot1x commands
All debug ip dhcp snooping commands
debug ip verify source packet
All debug platform commands

Show Commands

show archive log
show cable-diagnostics prbs
All show dot1x commands
show ip arp inspection
All show ip dhcp snooping commands
All show ip source binding commands
show ip verify source
All show ipv6 commands
All show platform commands
show table-map
Global Configuration Mode

All \texttt{dot1x} commands
All \texttt{event manager} commands
\texttt{exception crashinfo}
\texttt{errdisable detect cause dhcp-rate-limit}
\texttt{errdisable recovery cause dhcp-rate-limit}
\texttt{interface tunnel}
All \texttt{ip arp inspection} commands
All \texttt{ip dhcp snooping} commands
\texttt{ip source binding}
\texttt{ip sticky-arp}
All \texttt{macro auto} commands
\texttt{memory reserve critical}
\texttt{service compress-config}

Interface Configuration Mode

All \texttt{dot1x} commands
All \texttt{ip arp inspection} commands
All \texttt{ip dhcp snooping} commands
\texttt{ip sticky-arp ignore}
\texttt{ip tcp adjust-mss}
\texttt{ip verify source [tracking | vlan]}
\texttt{transmit-interface type number}