System Management Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches

First Published: July 2013
Lasted Updated: August 2014

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

Overview

This document describes how to configure system management features on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*. The switch can be managed through one of the following methods:

- Command Line Interface (CLI) over a serial connection to the switch console or over a telnet session
- Web management interface through a browser (Network Management)
- Network Management Application through SNMP

This document describes managing the switch using the CLI. The CLI interface supports the standard IOS commands.

Features

The switch ships with one of these software images installed:

- The LAN Base image includes advanced quality of service (QoS), flexible VLAN handling, supervisory control and data acquisition (SCADA) protocol classification support, resilient Ethernet protocol (REP) for improved convergence time in ring topologies, Flexlink for fast failover in hub-and-spoke topologies, and comprehensive security features.
- The IP Services image adds advanced Layer 3 features such as support for advanced IP routing protocols, Multi-VPN Routing and Forwarding Customer Edge (Multi-VRF CE/VRF-Lite), and Policy Based Routing (PBR).

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

The switch has two different types of interfaces by default: network node interfaces (NNIs) to connect to the service provider network and user network interfaces (UNIs) to connect to customer networks. Some features are supported only on one of these port types. You can also configure enhanced network interfaces (ENIs). An ENI is typically a user-network facing interface and has the same default configuration and functionality as UNIs, but can be configured to support protocol control packets for Cisco Discovery Protocol (CDP), Spanning-Tree Protocol (STP), Link Layer Discovery Protocol (LLDP), and EtherChannel Link Aggregation Control Protocol (LACP) or Port Aggregation Protocol (PAgP).

This chapter provides a summary of the following system management features:

DHCP

The initial switch configuration (for example, assigning the switch IP address and default gateway information) can be performed through the switch setup program, manually, or through a Dynamic Host Configuration Protocol (DHCP) server.

- Use the switch setup program if you want to be prompted for specific IP information.

  For more information about the setup program, see the "Configuring the Switch with the CLI-Based Setup Program" appendix in the *Cisco 1E 2000U Switch Hardware Installation Guide*.

- If you are an experienced user familiar with the switch configuration steps, use the CLI to manually configure the switch. Otherwise, use the switch setup program.
- Use a DHCP server for centralized control and automatic assignment of IP information after the server is configured.

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 the other is 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.

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.

Related Topics

Chapter 2, "Assigning the Switch IP Address and Default Gateway"

Switch Boot Optimization

You can configure the switch to minimize the time it takes to boot. When switch boot optimization is enabled, the switch disables the memory test, file system check (FSCK), and power-on self-test (POST) that occur during the normal boot process.

Related Topics

Chapter 3, "Configuring Switch Boot Optimization"

NTP

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.

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

Related Topics

Chapter 4, "Administering the Switch"

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.

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.

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.

Related Topics

Chapter 4, "Administering the Switch"

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.

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.

Related Topics

Chapter 4, "Administering the Switch"

Switch Alarms

The switch software monitors switch conditions on a per-port or a switch basis. If the conditions present on the switch or a port do not match the set parameters, the switch software triggers an alarm or a system message. By default, the switch software sends the system messages to a system message logging facility, or a *syslog* facility. You can also configure the switch to send Simple Network Management Protocol (SNMP) traps to an SNMP server. You can configure the switch to trigger an external alarm device by using the alarm relay.

Related Topics

Chapter 5, "Configuring the Switch Alarms"

SDM Templates

If the switch is running the IP services image, you can use SDM templates 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 Ternary Content Addressable Memory (TCAM) resources to support different features. You can use the SDM templates for IP Version 4 (IPv4) and select the default template to balance system resources or select the layer-2 template to support only Layer 2 features in hardware.

Note Switches running the LAN Base image support only the layer-2 template

The dual IPv4 and IPv6 templates also enable a dual stack environment.

Related Topics

Chapter 6, "Configuring SDM Templates"

Smartports Macros

Smartports macros provide a convenient way to save and share common configurations. You can use Smartports macros to enable features and settings based on the location of a switch in the network and for mass configuration deployments across the network.

Each Smartports macro is a set of CLI commands. The switch software has a set of default macros (which cannot be edited by user). You can also create your own macros. Smartports macros do not contain new CLI commands; they are simply a group of existing CLI commands.

Related Topics

Chapter 7, "Configuring Smartports Macros"

LLDP and LLDP-MED

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 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 (PoE), and inventory management.

Related Topics

Chapter 8, "Configuring LLDP and LLDP-MED"

Port-Based Traffic Control

The switch has the following features for controlling traffic on an interface:

- Storm control—Prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces
- Protected ports—Ensures that there is no exchange of unicast, broadcast, or multicast traffic between these ports on the switch
- Port blocking—Blocks a port (protected or nonprotected) from flooding unknown unicast or multicast packets to other ports
- Port security—Restricts input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port

Related Topics

Chapter 9, "Configuring Port-Based Traffic Control"

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.

Related Topics

Chapter 10, “Configuring CDP”

SPAN and RSPAN

You can analyze network traffic passing through ports or VLANs by using Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer or other monitoring or security device. SPAN copies (or mirrors) traffic received or sent (or both) on source ports or source VLANs to a destination port for analysis. SPAN does not affect the switching of network traffic on the source ports or VLANs. You must dedicate the destination port for SPAN use. Except for traffic that is required for the SPAN or RSPAN session, destination ports do not receive or forward traffic.

Related Topics

Chapter 11, “Configuring SPAN and RSPAN”

RMON

Remote Network Monitoring (RMON) is a standard monitoring specification that defines a set of statistics and functions that can be exchanged between RMON-compliant console systems and network probes. RMON provides you with comprehensive network-fault diagnosis, planning, and performance-tuning information. You can use the RMON feature with the Simple Network Management Protocol (SNMP) agent in the switch to monitor all the traffic flowing among switches on all connected LAN segments.

Related Topics

Chapter 12, “Configuring RMON”

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. You can use system message logging in the following ways:

- Set the severity level of the messages to control the type of messages displayed on the consoles and each of the destinations.
- Time-stamp log messages or set the syslog source address to enhance real-time debugging and management.
- 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.
- Remotely monitor system messages by viewing the logs on a syslog server or by accessing the switch through Telnet or through the console port.

Related Topics

Chapter 13, "Configuring System Message Logging"

SNMP

Simple Network Management Protocol (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.

Related Topics

Chapter 14, "Configuring SNMP"

Cisco IOS IP SLAs

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.

Related Topics

Chapter 16, "Configuring Cisco IOS IP SLAs Operations"

Embedded Event Manager

Embedded Event Manager (EEM) is a distributed and customized approach to event detection and recovery within a Cisco IOS device. EEM offers the ability to monitor events and take informational, corrective, or any other EEM action when the monitored events occur or when a threshold is reached. An EEM policy defines an event and the actions to be taken when that event occurs.

This policy is a programmed script that you can use to customize a script to invoke an action based on a given set of events occurring. The script generates actions such as generating custom syslog or Simple Network Management Protocol (SNMP) traps, invoking CLI commands, forcing a failover, and so forth. The event management capabilities of EEM are useful because not all event management can be

managed from the switch and because some problems compromise communication between the switch and the external network management device. Network availability is improved if automatic recovery actions are performed without rebooting the switch.

Related Topics

Chapter 15, "Configuring Embedded Event Manager"

Ethernet OAM, CFM, and E-LMI

Ethernet Operations, Administration, and Maintenance (OAM) is a protocol for installing, monitoring, and troubleshooting Ethernet networks to increase management capability within the context of the overall Ethernet infrastructure. The switch supports IEEE 802.1ag Connectivity Fault Management (CFM), Ethernet Local Management Interface (E-LMI), and IEEE 802.3ah Ethernet OAM discovery, link monitoring, remote fault detection, and remote loopback. It also supports IP Service Level Agreements (SLAs) for CFM, and ITU-T Y.1731 fault management. Ethernet OAM manager controls the interworking between any two of the protocols (CFM, E-LMI, and OAM).

Related Topics

Chapter 17, "Configuring Ethernet OAM, CFM, and E-LMI"

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

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.
- Health monitoring runs in the background.

Related Topics

Chapter 18, "Configuring Online Diagnostics"

Supported MIBs

See Appendix A, "Supported MIBs" for the list of supported management information bases (MIBs) for this release.

Assigning the Switch IP Address and Default Gateway

This chapter describes how to create the initial switch configuration for the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*. Initial configuration involves assigning the switch IP address and default gateway information by using a variety of automatic and manual methods. This chapter also describes how to modify the switch startup configuration.

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 2-25.

This chapter includes the following sections:

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

Information About Assigning Switch Information

This section describes the processes involved in initial configuration of switch information and includes the following topics:

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.

Note For information about the Switch Boot Optimization feature, which minimizes switch boot time, see Chapter 3, "Configuring Switch Boot Optimization."

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 switch has a removable compact flash card that stores the Cisco IOS software image and configuration files. You can replace and upgrade the switch without reconfiguring it. Removing the compact flash card does not interrupt switch operation. When the compact flash card is removed, you do not have access to the flash file system, and any attempt to access it generates an error message. The switch ships with the compact flash memory card installed and supports any size compact flash card.

Use the **show flash:** privileged EXEC command to display the compact flash file settings.

For information about how to remove or replace the compact flash memory card on the switch, see the *Cisco IE 2000U Switch Hardware Installation Guide*.

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 Software Failure" section and the "Recovering from a Lost or Forgotten Password" section in the "Troubleshooting" chapter in the *Cisco IOS Basics and File Management for Connected Grid Switches*.

Note You can interrupt the automatic boot process by pressing the break key on the console after the flash file system has initialized. If you configured the switch to manually boot from the boot loader mode, you cannot use the break key to interrupt the boot process. The default configuration is the automatic boot process. For more information, see the command reference listed in the "Related Documents" section on page 2-25.

Note You can disable password recovery. For more information, see the "Disabling Password Recovery" section in the *Cisco Connected Grid Switches Security Software Configuration Guide*.

DHCP-Based Autoconfiguration

Dynamic Host Configuration Protocol (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.

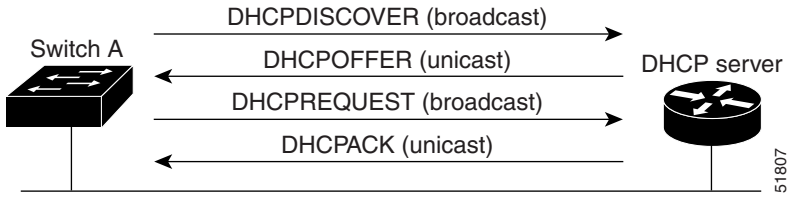
DHCP-based autoconfiguration replaces the BOOTP client functionality on your switch.

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 2-1 shows the sequence of messages that are exchanged between the DHCP client and the DHCP server.

Figure 2-1 DHCP Client and Server Message Exchange



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 "TFTP Server" section on page 2-5.

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

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

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

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

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

DHCP Image Upgrade

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).

  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 *IP Addressing: DHCP Configuration Guide, Cisco IOS Release 15M&T*.

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.

TFTP Server

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

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

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

- The configuration file named in the DHCP reply (the actual switch configuration file).
- The network-confg or the cisconet.cfg file (known as the default configuration files).
- The router-confg 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 "Relay Device" section on page 2-6. The preferred solution is to configure the DHCP server with all the required information.

DNS Server

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.

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 2-2, configure the router interfaces as follows:

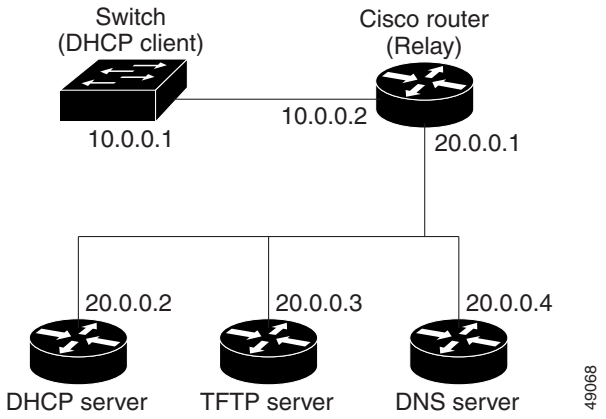
On interface 10.0.0.2:

```
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
```

Figure 2-2 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-confg or cisconet.cfg default configuration file. (If the network-confg file cannot be read, the switch reads the cisconet.cfg file.)

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

  After obtaining its hostname from the default configuration file or the DHCP reply, the switch reads the configuration file that has the same name as its hostname (*hostname*-confg or *hostname*.cfg, depending on whether network-confg 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-confg, cisconet.cfg, or the hostname file, it reads the router-confg file. If the switch cannot read the router-confg file, it reads the ciscortr.cfg file.

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

Example Configuration

Figure 2-3 shows a sample network for retrieving IP information by using DHCP-based autoconfiguration.

Figure 2-3 DHCP-Based Autoconfiguration Network Example

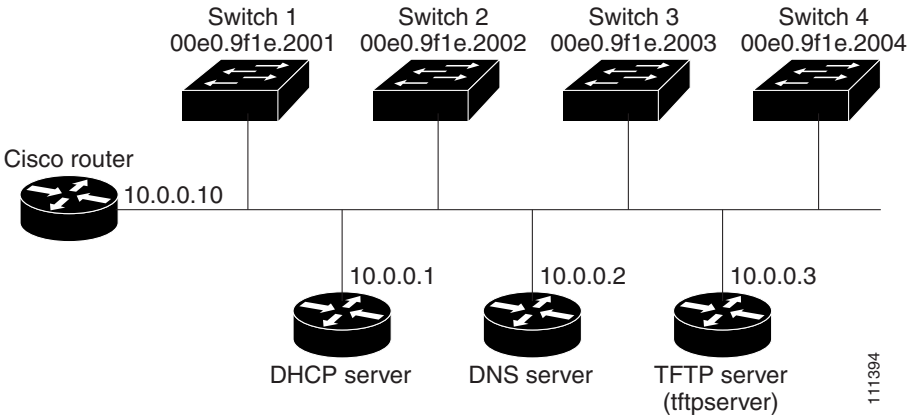


Table 2-1 shows the configuration of the reserved leases on the DHCP server.

Table 2-1 DHCP Server Configuration

	Switch A	Switch B	Switch C	Switch D
Binding key (hardware address)	00e0.9f1e.2001	00e0.9f1e.2002	00e0.9f1e.2003	00e0.9f1e.2004
IP address	10.0.0.21	10.0.0.22	10.0.0.23	10.0.0.24
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Router address	10.0.0.10	10.0.0.10	10.0.0.10	10.0.0.10
DNS server address	10.0.0.2	10.0.0.2	10.0.0.2	10.0.0.2
TFTP server name	*tftpserver* or *10.0.0.3*	*tftpserver* or *10.0.0.3*	*tftpserver* or *10.0.0.3*	*tftpserver* or *10.0.0.3*
Boot filename (configuration file) (optional)	switcha-confg	switchb-confg	switchc-confg	switchd-confg
Hostname (optional)	switcha	switchb	switchc	switchd

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-confg file used in the two-file read method. This file contains the hostname to be assigned to the switch based on its IP address. The base directory also contains a configuration file for each switch (*switcha-confg*, *switchb-confg*, and so forth) as shown in this display:

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

DHCP Client Configuration

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

Configuration Explanation

In Figure 2-3, Switch A reads its configuration file as follows:

- It obtains its IP address 10.0.0.21 from the DHCP server.
- If no configuration filename is given in the DHCP server reply, Switch A reads the network-confg file from the base directory of the TFTP server.
- It adds the contents of the network-confg file to its host table.
- It reads its host table by indexing its IP address 10.0.0.21 to its hostname (switcha).
- It reads the configuration file that corresponds to its hostname; for example, it reads *switch1-confg* from the TFTP server.

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

Prerequisites

- 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.
- If you are using DHCP to relay the configuration file location on the network, determine if you need to configure a Trivial File Transfer Protocol (TFTP) server and a Domain Name System (DNS) server.
- If the DHCP server is running on a different LAN than the switch, you should configure a DHCP relay device between your switch and the DHCP server.

Guidelines and Limitations

Guidelines for using DCHP to assign switch information are described in the following sections.

DHCP-Based Autoconfiguration

- 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 if 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.

DHCP Server

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 *IP Addressing: DHCP Configuration Guide, Cisco IOS Release 15M&T*.

Default Settings

Feature	Default Setting
IP address and subnet mask	No IP address or subnet mask are defined.
Default gateway	No default gateway is defined.
Enable secret password	No password is defined.
Hostname	The factory-assigned default hostname is *Switch*.
Telnet password	No password is defined.

Feature	Default Setting
Default Boot Configuration	
Operating system software image	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.
Configuration file	Configured switches use the *config.text* file stored on the system board in flash memory. A new switch has no configuration file.

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.

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

If you are an experienced user familiar with the switch configuration steps, manually configure the switch. Otherwise, use the setup program described previously.

This section includes the following topics:

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.

If your DHCP server is a Cisco device, see the *IP Addressing: DHCP Configuration Guide, Cisco IOS Release 15M&T* for additional information about configuring DHCP.

This section includes the following topics:

Configuring DHCP Autoconfiguration (Only Configuration File)

Follow this procedure to configure DHCP autoconfiguration of the TFTP and DHCP settings on a new switch to download a new configuration file.

BEFORE YOU BEGIN

Review the "Prerequisites" section on page 2-9 and "Guidelines and Limitations" section on page 2-9.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip dhcp pool** *poolname*	Create a name for the DHCP Server address pool, and enter DHCP pool configuration mode.
Step 3	**bootfile** *filename*	Specify the name of the configuration file that is used as a boot image.
Step 4	**network** *network-number mask prefix-length*	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 (/).
Step 5	**default-router** *address*	Specify the IP address of the default router for a DHCP client.
Step 6	**option 150** *address*	Specify the IP address of the TFTP server.
Step 7	**exit**	Return to global configuration mode.
Step 8	**tftp-server flash:***filename.text*	Specify the configuration file on the TFTP server.
Step 9	**interface** *interface-id*	Specify the address of the client that will receive the configuration file.
Step 10	**no switchport**	Put the interface into Layer 3 mode.
Step 11	**ip address** *address mask*	Specify the IP address and mask for the interface.

	Command	Purpose
Step 12	**end**	Return to privileged EXEC mode.
Step 13	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

This example shows how to configure a switch as a DHCP server to download a configuration file:

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

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

Follow this procedure 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 YOU BEGIN

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.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip dhcp pool** *name*	Create a name for the DHCP server address pool and enter DHCP pool configuration mode.
Step 3	**bootfile** *filename*	Specify the name of the file that is used as a boot image.
Step 4	**network** *network-number mask prefix-length*	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 (/).
Step 5	**default-router** *address*	Specify the IP address of the default router for a DHCP client.
Step 6	**option 150** *address*	Specify the IP address of the TFTP server.
Step 7	**option 125** *hex*	Specify the path to the text file that describes the path to the image file.
Step 8	**copy tftp flash** *filename.txt*	Upload the text file to the switch.

	Command	Purpose
Step 9	**copy tftp flash** *imagename.tar*	Upload the tarfile for the new image to the switch.
Step 10	**exit**	Return to global configuration mode.
Step 11	**tftp-server flash:***config.text*	Specify the Cisco IOS configuration file on the TFTP server.
Step 12	**tftp-server flash:***imagename.tar*	Specify the image name on the TFTP server.
Step 13	**tftp-server flash:***filename.txt*	Specify the text file that contains the name of the image file to download
Step 14	**interface** *interface-id*	Specify the address of the client that will receive the configuration file.
Step 15	**no switchport**	Put the interface into Layer 3 mode.
Step 16	**ip address** *address mask*	Specify the IP address and mask for the interface.
Step 17	**end**	Return to privileged EXEC mode.
Step 18	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

This example shows how to configure a switch as a DHCP server to download a configuration file and image:

```
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
0000.0009.0a05.08661.7574.6f69.6e73.7461.6c6c.5f64.686370
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 gigabitEthernet1/0/4
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1 255.255.255.0
Switch(config-if)# end
```

Configuring the Client

Follow this procedure to configure a switch to download a configuration file and new image from a DHCP server.

BEFORE YOU BEGIN

Review the "Prerequisites" section on page 2-9 and "Guidelines and Limitations" section on page 2-9.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**boot host dhcp**	Enable autoconfiguration with a saved configuration.
Step 3	**boot host retry timeout** *timeout-value*	(Optional) Set the amount of time the system tries to download a configuration file. **Note** If you do not set a timeout the system will indefinitely try to obtain an IP address from the DHCP server.
Step 4	**banner config-save ^C** *warning-message* **^C**	(Optional) Create warning messages to be displayed when you try to save the configuration file to NVRAM.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show boot**	Verify the configuration.

EXAMPLE

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)
Switch#
```

Note You should only configure and enable the Layer 3 interface. Do not assign an IP address or DHCP-based autoconfiguration with a saved configuration.

Manually Assigning IP Information

BEFORE YOU BEGIN

Review the "Assigning Switch Information" section on page 2-11.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface vlan** *vlan-id*	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.
Step 3	**ip address** *ip-address subnet-mask*	Enter the IP address and subnet mask.
Step 4	**exit**	Return to global configuration mode.
Step 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.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show interfaces vlan** *vlan-id*	Verify the configured IP address.
Step 8	**show ip redirects**	Verify the configured default gateway.
Step 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 4, "Administering the Switch."

EXAMPLE

```
Switch(config)# interface vlan 100
Switch(config-if)# ip address 172.20.137.50 255.255.255.0
Switch(config-if)# ip default-gateway 172.20.137.1
Switch(config-if)# exit
```

Modifying the Startup Configuration

See also *Cisco IOS Basics and File Management for Cisco IE 2000U and Connected Grid Switches* for information about switch configuration files.

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 "DHCP-Based Autoconfiguration" section on page 2-3.

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.

BEFORE YOU BEGIN

Review the "Boot Process" section on page 2-2.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
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.

EXAMPLE

```
Switch(config)# boot config-file flash:config1.text
Switch(config)# end
```

Booting Manually

By default, the switch automatically boots; however, you can configure it to manually boot.

BEFORE YOU BEGIN

Review the "Boot Process" section on page 2-2.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**boot manual**	Enable the switch to manually boot during the next boot cycle.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show boot**	Verify your entries. The **boot manual** global command changes the setting of the MANUAL_BOOT environment variable. The next time you reboot the system, the switch is in boot loader mode, as shown by the *switch:* prompt. To boot the system, use the **boot** *filesystem***:/***file-url* boot loader command. • For *filesystem***:**, use **flash:** for the system board flash device. • For *file-url*, specify the path (directory) and the name of the bootable image. Filenames and directory names are case sensitive.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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

EXAMPLE

```
Switch(config)# boot manual
Switch(config)# end
```

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.

BEFORE YOU BEGIN

Review the "Boot Process" section on page 2-2.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**boot system** *filesystem***:/***file-url*	Configure the switch to boot a specific image in flash memory during the next boot cycle. • For *filesystem***:**, use **flash:** for the system board flash device. • For *file-url*, specify the path (directory) and the name of the bootable image. Filenames and directory names are case sensitive.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show boot**	Verify your entries. The **boot system** global command changes the setting of the BOOT environment variable. During the next boot cycle, the switch attempts to automatically boot the system using information in the BOOT 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 system** global configuration command.

EXAMPLE

```
Switch(config)# boot system flash:/images/new-ios-image
Switch(config)# end
```

Controlling Environment Variables

With a normally operating switch, you enter 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.
```

Note You can interrupt the automatic boot process by pressing the break key on the console after the flash file system has initialized. If you configured the switch to manually boot from boot loader mode, you cannot use the break key to interrupt the boot process. The default configuration is the automatic boot process. For more information, see the command reference listed in the "Related Documents" section on page 2-25.

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 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 view this table, see:

http://www.cisco.com/en/US/customer/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 listed in the "Related Documents" section on page 2-25.

Table 2-2 describes the function of the most common environment variables.

Table 2-2 Environment Variables

Variable	Boot Loader Command	Cisco IOS Global Configuration Command
BOOT	**set BOOT** *filesystem***:/***file-url ...* 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 file 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.	**boot system** *filesystem:/file-url ...* Specifies the Cisco IOS image file to load during the next boot cycle. This command changes the setting of the BOOT environment variable.
MANUAL_BOOT	**set MANUAL_BOOT yes** 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 boot loader mode.	**boot manual** 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.
CONFIG_FILE	**set CONFIG_FILE flash:/***file-url* Changes the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.	**boot config-file flash:/***file-url* 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.

Configuring a Scheduled 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.

BEFORE YOU BEGIN

Follow these guidelines when using the **reload** command:

- 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 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.

DETAILED STEPS

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

- **[warm] reload in** [*hh***:**]*mm* [*text*]

  This command schedules a reload or warm reload of the software to take affect at 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 long.

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

  This command schedules a reload or warm 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.

You can use the **warm** keyword to reload the switch without reading images from storage. The Cisco IOS image reboots without ROM monitor mode (ROMMON) intervention. It restores the read-write data from a previously saved copy in the RAM and starts without copying the image from flash memory to RAM or self-decompression of the image. Thus, the switch reboots much faster.

Note The **warm** keyword causes the switch to boot automatically, even if your switch is configured for manual booting.

EXAMPLE

This example shows how to reload the switch software on the current day at 19:30:

```
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 schedule a warm reload of the switch software at a future time:

```
Switch# warm 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).

Verifying Configuration

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

```
IE-2000U-4T#show running-config
Building configuration...

Current configuration : 3018 bytes
!
! Last configuration change at 02:55:14 UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname IE-2000U-4T
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
system mtu routing 1998
ip routing
no ip domain-lookup
ip name-server 10.78.134.231
!
ip dhcp relay information policy keep
ip dhcp relay information trust-all
!
ip dhcp pool test1
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 10.78.134.231
.
.
.
```

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 the *Cisco IOS Basics and File Management for Cisco IE 2000U and Connected Grid Switches*.

Configuration Example

This example shows how to configure a switch as a DHCP server to download a configuration file:

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

This example shows how to configure a switch as a DHCP server to download a configuration file and image:

```
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
0000.0009.0a05.08661.7574.6f69.6e73.7461.6c6c.5f64.686370
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 gigabitEthernet1/0/4
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1 255.255.255.0
Switch(config-if)# end
```

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

```
Switch# configure terminal
Switch(conf)# boot host dhcp
Switch(conf)# boot host retry timeout 300
Switch(conf)# 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)
Switch#
```

This example shows how to reload the switch software on the current day at 19:30:

```
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 schedule a warm reload of the switch software at a future time:

```
Switch# warm 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]
```

Related Documents

- Cisco IOS Configuration Fundamentals Command Reference, Release 15.2M&T
- Cisco IOS IP Addressing Services Command Reference, Release 15.2M&T
- IP Addressing: DHCP Configuration Guide, Cisco IOS Release 15M&T
- Cisco Connected Grid Switches Security Software Configuration Guide
- Cisco IOS Basics and File Management for Connected Grid Switches
- Cisco IE 2000U Switch Hardware Installation Guide

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

Configuring Switch Boot Optimization

This chapter describes how to configure the Switch Boot Optimization feature for Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*.

This chapter includes the following sections:

Information About Switch Boot Optimization

The normal switch boot process involves a memory test, file system check (FSCK), and power-on self-test (POST). For details about the normal boot process, see the "Boot Process" section on page 2-2.

The **boot fast** command in global configuration mode minimizes switch boot time by disabling these tests.

If the system crashes when **boot fast** is enabled, reload sequences occur immediately if your switch is set up to automatically bring up the system by using information in the BOOT environment variable. Otherwise, these reload sequences occur after you enter the manual boot command in bootloader configuration mode.

First Reload

The switch disables the boot fast feature and displays the following warning message:

```
"Saving the crash information to flash.
Reloading with boot fast feature disabled..."
```

After the system message appears, the system saves the crash information and automatically resets itself for the next reload cycle.

Second Reload

The boot loader performs its normal full memory test and FSCK check with LED status progress. If the memory and FSCK tests are successful, the system performs additional POST tests and the results are displayed on the console.

After the system comes up successfully, the boot fast feature is reenabled.

Prerequisites

Review the "Information About Switch Boot Optimization" section on page 3-1 and "Guidelines and Limitations" section on page 3-2.

Guidelines and Limitations

Caution The system requires the memory test, file system check, and POST to function properly. Enabling switch boot optimization might lead to uncertain system behavior.

Default Settings

By default, **boot fast** is disabled.

Configuring Switch Boot Optimization

To enable the switch boot optimization feature, enter the following global configuration command:

boot fast

To disable the switch boot optimization feature, enter the following command:

no boot fast

Verifying Configuration

Command	Purpose
show boot	Displays information about the switch boot optimization configuration.

Configuration Example

This example shows how to enable, disable, and verify the switch boot optimization configuration:

```
Switch#conf t
Switch(config)#boot fast
Switch(config)#end
Switch#sh boot
Boot optimization   : enabled


Switch#conf t
Switch(config)#no boot fast
Switch(config)#end
Switch#sh boot
Boot optimization   : disabled
```

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520	Cisco IOS Release 15.0(2)ED
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 15.0(2)ED

Administering the Switch

This chapter describes how to perform one-time operations to administer the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*.

This chapter includes the following sections:

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 4-38.

Information About Administering the Switch

This section includes the following topics about administering the switch:

- ARP Table, page 4-5

System Clock

The system 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 set the time zone and adjust for Daylight Saving Time (DST), also known as summer time.

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 4-15.

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.

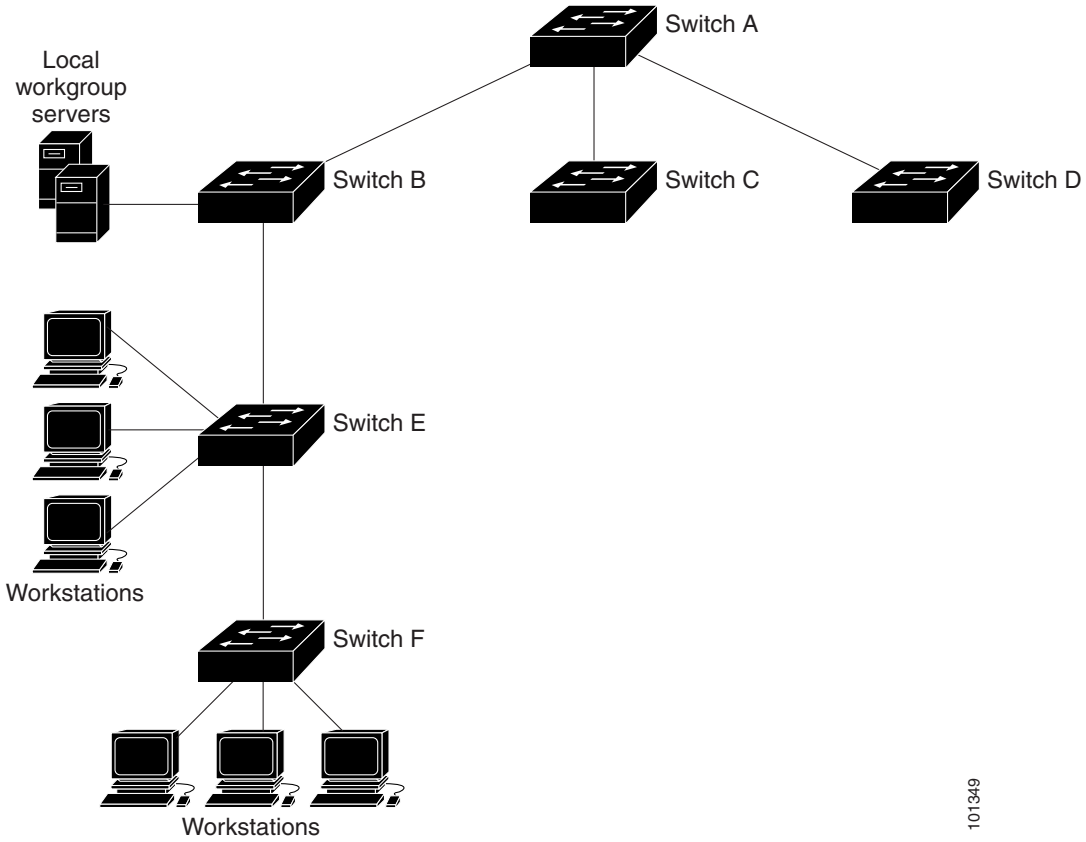
The communications between devices running NTP (known as *associations*) are usually statically configured; each device is given the IP address of all devices with which it should form associations. Accurate timekeeping is possible by exchanging NTP messages between each pair of devices with an association. 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 4-1 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 4-1 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 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 also allows host systems to be time-synchronized.

DNS

The DNS protocol controls the Domain Name System (DNS), which is a distributed database for mapping 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 use period delimiters. 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 track 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.

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).

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.

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

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

For more information about private VLANs, see the "Configuring Private VLANs" chapter in the *Layer 2 Switching Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*.

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. See the "Disabling MAC Address Learning on a VLAN" section on page 4-33 for more information.

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 802 networks other than Ethernet is specified by the Subnetwork Access Protocol (SNAP). By default, standard Ethernet-style ARP encapsulation (represented by the **arpa** keyword) is enabled on the IP interface.

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

For CLI procedures, see the *IP Addressing: ARP Configuration Guide, Cisco IOS Release 15M&T*.

Prerequisites

You should have at least a basic familiarity with the Cisco IOS environment and the command-line interface.

Guidelines and Limitations

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.

MAC Address Table

See the "Configuring Unicast MAC Address Filtering" section on page 4-32 and "Disabling MAC Address Learning on a VLAN" section on page 4-33.

Default Settings

Feature	Default Setting
NTP	
NTP	Enabled on all interfaces. All interfaces receive NTP packets.
NTP authentication	Disabled. No authentication key is specified.
NTP peer or server associations	None configured.
NTP broadcast service	Disabled; no interface sends or receives NTP broadcast packets.
NTP access restrictions	No access control is specified.
NTP packet source IP address	The source address is set by the outgoing interface.
System Name	
System name and prompt	The default switch system name and prompt is *Switch*.
DNS	
DNS enable state	Enabled.
DNS default domain name	None configured.
DNS servers	No name server addresses are configured.
Banners	
Message-of-the-day (MOTD) and login banners	No banners are configured.
MAC Address Table	
Aging time	300 seconds.
Dynamic addresses	Automatically learned.
Static addresses	None configured.

Configuring NTP

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 manual configuration, see the "Configuring Time and Date Manually" section on page 4-15.

This section includes the following topics:

Configuring NTP Authentication

Follow this procedure to authenticate the associations (communications between devices running NTP that provide for accurate timekeeping) with other devices for security purposes.

BEFORE YOU BEGIN

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.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ntp authenticate**	Enable the NTP authentication feature, which is disabled by default.
Step 3	**ntp authentication-key** *number* **md5** *value*	Define the authentication keys. By default, none are defined. • For *number*, specify a key number. The range is 1 to 4294967295. • **md5** specifies that message authentication support is provided by using the message digest algorithm 5 (MD5). • For *value*, enter an arbitrary string of up to eight characters for the key. The switch does not synchronize to a device unless both have one of these authentication keys, and the key number is specified by the **ntp trusted-key** *key-number* command.

	Command	Purpose
Step 4	**ntp trusted-key** *key-number*	Specify one or more key numbers (defined in Step 3) that a peer NTP device must provide in its NTP packets for this switch to synchronize to it. By default, no trusted keys are defined. For *key-number*, specify the key defined in Step 3. This command provides protection against accidentally synchronizing the switch to a device that is not trusted.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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

EXAMPLE

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).

BEFORE YOU BEGIN

Review the "Network Time Protocol" section on page 4-2.

DETAILED STEPS

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

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

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

EXAMPLE

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.

Configuring the Switch to Send NTP Broadcast Packets

BEFORE YOU BEGIN

Review the "Network Time Protocol" section on page 4-2.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface to send NTP broadcast packets, and enter interface configuration mode.
Step 3	**no shutdown**	Enable the port, if necessary. By default, user network interfaces (UNIs) and enhanced network interfaces (ENIs) are disabled, and network node interfaces (NNIs) are enabled.
Step 4	**ntp broadcast** [**version** *number*] [**key** *keyid*] [*destination-address*]	Enable the interface to send NTP broadcast packets to a peer. By default, this feature is disabled on all interfaces. • (Optional) For *number*, specify the NTP version number. The range is 1 to 3. If you do not specify a version, Version 3 is used. • (Optional) For *keyid*, specify the authentication key to use when sending packets to the peer. • (Optional) For *destination-address*, specify the IP address of the peer that is synchronizing its clock to this switch.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.
Step 8		Configure the connected peers to receive NTP broadcast packets as described in the next procedure.

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

EXAMPLE

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
```

Configuring the Switch to Receive NTP Broadcast Packets

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface to receive NTP broadcast packets, and enter interface configuration mode.
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and enhanced network interfaces (ENIs) are disabled, and NNIs are enabled.
Step 4	**ntp broadcast client**	Enable the interface to receive NTP broadcast packets. By default, no interfaces receive NTP broadcast packets.
Step 5	**exit**	Return to global configuration mode.
Step 6	**ntp broadcastdelay** *microseconds*	(Optional) Change the estimated round-trip delay between the switch and the NTP broadcast server. The default is 3000 microseconds; the range is 1 to 999999.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show running-config**	Verify your entries.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable 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.

EXAMPLE

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

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

Configuring NTP Access Restrictions

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

- Creating an Access Group and Assigning a Basic IP Access List, page 4-12

- Disabling NTP Services on a Specific Interface, page 4-13

Creating an Access Group and Assigning a Basic IP Access List

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.

BEFORE YOU BEGIN

Review the "Network Time Protocol" section on page 4-2.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
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.

	Command	Purpose
Step 3	**access-list** *access-list-number* **permit** *source* [*source-wildcard*]	Create the access list. • For *access-list-number*, enter the number specified in Step 2. • Enter the **permit** keyword to permit access if the conditions are matched. • For *source*, enter the IP address of the device that is permitted access to the switch. • (Optional) For *source-wildcard*, enter the wildcard bits to be applied to the source. **Note** When creating an access list, remember that, by default, the end of the access list contains an implicit deny statement for everything if it did not find a match before reaching the end.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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

EXAMPLE

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.

BEFORE YOU BEGIN

Review the "Network Time Protocol" section on page 4-2.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and specify the interface to disable.

	Command	Purpose
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and enhanced network interfaces (ENIs) are disabled, and NNIs are enabled.
Step 4	**ntp disable**	Disable NTP packets from being received on the interface. By default, all interfaces receive NTP packets.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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

EXAMPLE

```
Switch(config)# interface ethernet 0
Switch(config-if)# ntp disable
Switch(config-if)# end
```

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.

BEFORE YOU BEGIN

Review the "Network Time Protocol" section on page 4-2.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ntp source** *interface type interface number*	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.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

The specified interface is used for the source address for all packets sent to all destinations. If a source address is to be used for a specific association, use the **source** keyword in the **ntp peer** or **ntp server** global configuration command as described in the "Configuring NTP Associations" section on page 4-8.

EXAMPLE

The following example shows how to configure a switch to use the IPv4 or IPv6 address of Ethernet interface 0 as the source address of all outgoing NTP packets:

```
Switch(config)# ntp source ethernet 0
```

Configuring Time and Date Manually

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

This section includes the following topics:

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.

BEFORE YOU BEGIN

Review the "System Clock" section on page 4-2.

DETAILED STEPS

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

EXAMPLE

This example shows how to manually set the system clock to 1:32 p.m. on July 23, 2014:

```
Switch# clock set 13:32:00 23 July 2014
```

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

BEFORE YOU BEGIN

Obtain your time zone information.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**clock timezone** *zone hours-offset* [*minutes-offset*]	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. • For *zone*, enter the name of the time zone to be displayed when standard time is in effect. The default is UTC. • For *hours-offset*, enter the hours offset from UTC. • (Optional) For *minutes-offset*, enter the minutes offset from UTC.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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

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

EXAMPLE

The following example sets the time zone to Pacific Standard Time (PST), which is 8 hours behind UTC:

```
Switch(config)# clock timezone PST -8
```

Configuring Daylight Saving Time (Summer Time)

Recurring Daylight Saving Time

Follow this procedure to configure daylight saving time (summer time) in areas where it starts and ends on a particular day of the week each year.

The first part of the **clock summer-time** global configuration command specifies when DST 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 DST. If the starting month is after the ending month, the system assumes that you are in the southern hemisphere.

BEFORE YOU BEGIN

Obtain the DST information for your time zone.

DETAILED STEPS

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

EXAMPLE

This example shows how to specify that DST 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
```

Specific Dates for Daylight Saving Time

Follow this procedure if summer time in your area does not follow a recurring pattern (configure the exact date and time of the next summer time events):

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.

BEFORE YOU BEGIN

Obtain the daylight saving time information for your time zone.

DETAILED STEPS

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

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

EXAMPLE

This example shows how to set summer time to start on October 12, 2014, at 02:00, and end on April 26, 2015, at 02:00:

```
Switch(config)# clock summer-time pdt date 12 October 2014 2:00 26 April 2015 2:00
```

Configuring a System Name and Prompt

You configure the system name on the switch to identify it. When you set the system name, it is also used as the system prompt. 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.

BEFORE YOU BEGIN

Follow these guidelines when configuring the system name:

- Conventions dictate that computer names appear all lowercase.

- The name must follow the rules for ARPANET hostnames. They must start with a letter, end with a letter or digit, and contain only letters, digits, and hyphens. Names must be 63 characters or fewer. Creating an all numeric hostname is not recommended but the name will be accepted after an error is returned.
- A hostname of less than 10 characters is recommended.
- On most systems, a field of 30 characters is used for the hostname and the prompt in the CLI. Note that the length of your hostname may cause longer configuration mode prompts to be truncated.

DETAILED STEPS

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

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

EXAMPLE

```
Switch(config)# hostname ie2000u-1
```

Configuring DNS

If you use the switch IP address as its hostname, no DNS query occurs. If you configure a hostname that contains no periods (.), the system appends a period followed by the default domain name 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.

BEFORE YOU BEGIN

Obtain the DNS server IP address(es).

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip domain-name** *name*	Define a default domain name that the software uses to complete unqualified hostnames (names without a dotted-decimal domain name). **Note** Do not include the initial period that separates an unqualified name from the domain name. At system boot up, 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).
Step 3	**ip name-server** *server-address1* [*server-address2 ... server-address6*]	Specify the address of one or more name servers to use for name and address resolution. You can specify up to six name servers. Separate each server address with a space. The first server specified is the primary server. The switch sends DNS queries to the primary server first. If that query fails, the backup servers are queried.
Step 4	**ip domain-lookup**	(Optional) Enable DNS-based hostname-to-address translation on your switch. This feature is enabled by default. If your network devices require connectivity with devices in networks where you do not control name assignment, you can dynamically assign device names that uniquely identify your devices by using the global Internet naming scheme (DNS).
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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.

EXAMPLE

```
Switch(config)# ip domain-name cisco.com
Switch(config)# ip name-server 172.16.1.111 172.16.1.2
Switch(config)# end
```

Creating a Banner

You can configure a message-of-the-day (MOTD) and a login banner. The MOTD banner is displayed 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 is also displayed on all connected terminals. It appears after the MOTD banner and before the login prompts.

This section includes the following topics:

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.

DETAILED STEPS

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

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

EXAMPLE

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 that appears on all connected terminals. This banner appears after the MOTD banner and before the login prompt.

DETAILED STEPS

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

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

EXAMPLE

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).

This section includes the following topics:

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.

BEFORE YOU BEGIN

Review the "MAC Address Table" section on page 4-4.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**mac address-table aging-time** [**0** | *10-1000000*] [**vlan** *vlan-id*]	Set the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. The range is 10 to 1000000 seconds. The default is 300. You can also enter 0, which disables aging. Static address entries are never aged or removed from the table. For *vlan-id*, valid IDs are 1 to 4094. Do not enter leading zeros.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show mac address-table aging-time**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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

EXAMPLE

The following example shows how to configure aging time to 300 seconds:

```
Switch(config)# mac-address-table aging-time 300
```

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.

BEFORE YOU BEGIN

Obtain the NMS name or address and the community string.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*	Specify the recipient of the trap message. • For *host-addr*, specify the name or address of the NMS. • Specify **traps** (the default) to send SNMP traps to the host. Specify **informs** to send SNMP informs to the host. • Specify the SNMP version to support. Version 1, the default, is not available with informs. • For *community-string,* specify the string to send with the notification operation. Though you can set this string by using the **snmp-server host** command, we recommend that you define this string by using the **snmp-server community** command before using the **snmp-server host** command. • For *notification-type*, use the **mac-notification** keyword.
Step 3	**snmp-server enable traps mac-notification change**	Enable the switch to send MAC address change notification traps to the NMS.
Step 4	**mac address-table notification change**	Enable the MAC address change notification feature.
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 Layer 2 interface on which to enable the SNMP MAC address notification trap.

	Command	Purpose
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.

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.

EXAMPLE

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.

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.

BEFORE YOU BEGIN

Obtain the NMS name or address and the community string.

DETAILED STEPS

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

To disable MAC address-move notification traps, use the **no snmp-server enable traps 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.

EXAMPLE

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.

BEFORE YOU BEGIN

Obtain the NMS name or address and the community string.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*	Specify the recipient of the trap message. • For *host-addr*, specify the name or address of the NMS. • Specify **traps** (the default) to send SNMP traps to the host. Specify **informs** to send SNMP informs to the host. • Specify the SNMP version to support. Version 1, the default, is not available with informs. • For *community-string,* specify the string to send with the notification operation. Though you can set this string by using the **snmp-server host** command, we recommend that you define this string by using the **snmp-server community** command before using the **snmp-server host** command. • For *notification-type*, use the **mac-notification** keyword.
Step 3	**snmp-server enable traps mac-notification threshold**	Enable the switch to send MAC threshold notification traps to the NMS.
Step 4	**mac address-table notification threshold**	Enable the MAC address threshold notification feature.

	Command	Purpose
Step 5	**mac address-table notification threshold** [**limit** *percentage*] | [**interval** *time*]	Enter the threshold value for the MAC address threshold usage monitoring. • (Optional) For **limit** *percentage*, specify the percentage of the MAC address table use; valid values are from 1 to 100 percent. The default is 50 percent. • (Optional) For **interval** *time*, specify the time between notifications; valid values are greater than or equal to 120 seconds. The default is 120 seconds.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show mac address-table notification threshold** **show running-config**	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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.

EXAMPLE

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 percent:

```
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.

When you configure a static MAC address in a private-VLAN primary or secondary VLAN, you should also configure the same static MAC address in all associated VLANs. Static MAC addresses configured in a private-VLAN primary or secondary VLAN are not replicated in the associated VLAN. For more information about private VLANs, see the "Configuring Private VLANs" chapter in the *Layer 2 Switching Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*.

BEFORE YOU BEGIN

Review the "MAC Address Table" section on page 4-4.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id*	Add a static address to the MAC address table. • 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. • 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. • 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.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show mac address-table static**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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.

EXAMPLE

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.

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.

BEFORE YOU BEGIN

Follow these guidelines when using this feature:

- Multicast MAC addresses, broadcast MAC addresses, and router MAC addresses are not supported. If you specify one of these addresses when entering the **mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** global configuration command, one of these messages appears:

```
% Only unicast addresses can be configured to be dropped

% CPU destined address cannot be configured as drop address
```

- Packets that are forwarded to the CPU are also not supported.
- If you add a unicast MAC address as a static address and configure unicast MAC address filtering, the switch either adds the MAC address as a static address or drops packets with that MAC address, depending on which command was entered last. The second command that you entered overrides the first command.

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

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

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**mac address-table static** *mac-addr* **vlan** *vlan-id* **drop**	Enable unicast MAC address filtering and configure the switch to drop a packet with the specified source or destination unicast static address. • For *mac-addr*, specify a source or destination unicast MAC address. Packets with this MAC address are dropped. • For *vlan-id*, specify the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094.
Step 3	**end**	Return to privileged EXEC mode.

	Command	Purpose
Step 4	**show mac address-table static**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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

EXAMPLE

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 BEGIN

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

- 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.
- Use caution before disabling MAC address learning on a VLAN with a configured switch virtual interface (SVI). The switch then floods all IP packets in the Layer 2 domain.
- You can disable MAC address learning on a single VLAN ID from 1 to 4094 (for example, **no mac address-table learning vlan 223**) or a range of VLAN IDs, separated by a hyphen or comma (for example, **no mac address-table learning vlan 1-10, 15**).
- We recommend that you disable MAC address learning only in VLANs with two ports. If you disable MAC address learning on a VLAN with more than two ports, every packet entering the switch is flooded in that VLAN domain.
- You cannot disable MAC address learning on a VLAN that is used internally by the switch. If the VLAN ID that you enter is an internal VLAN, the switch generates an error message and rejects the command. To view internal VLANs in use, enter the **show vlan internal usage** privileged EXEC command.
- If you disable MAC address learning on a VLAN configured as a private-VLAN primary VLAN, MAC addresses are still learned on the secondary VLAN that belongs to the private VLAN and are then replicated on the primary VLAN. If you disable MAC address learning on the secondary VLAN, but not the primary VLAN of a private VLAN, MAC address learning occurs on the primary VLAN and is replicated on the secondary VLAN.
- You cannot disable MAC address learning on an RSPAN VLAN. The configuration is not allowed.

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

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no mac address-table learning vlan** *vlan-id*	Disable MAC address learning on the specified VLAN or VLANs. You can specify a single VLAN ID or a range of VLAN IDs separated by a hyphen or comma. Valid VLAN IDs 1 to 4094. It cannot be an internal VLAN.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show mac address-table learning** [**vlan** *vlan-id*]	Verify the configuration.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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

EXAMPLE

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

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

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

Displaying Address Table Entries

Command	Description
show ip igmp snooping groups	Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.

Command	Description
show mac address-table dynamic	Displays only dynamic MAC address table entries.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table notification	Displays the MAC notification parameters and history table.
show mac address-table static	Displays only static MAC address table entries.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

Verifying Configuration

Command	Purpose
show ntp associations [**detail**]	Display NTP information.
show ntp status	Display NTP information.
show clock [**detail**]	Display the time and date configuration.
show running-config	Display the DNS configuration.

Configuration Example

System Time and Date

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
```

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
```

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
```

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

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

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
```

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
```

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
```

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
```

MOTD Banner

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:
```

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)#
```

MAC Address Table

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
```

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
```

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 percent:

```
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
```

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
```

This example shows how to enable unicast MAC address filtering and 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
```

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

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

Related Documents

- Cisco IOS Configuration Fundamentals Command Reference, Release 15.2M&T
- Cisco IOS Basic System Management Command Reference
- Cisco IOS IP Addressing Services Command Reference, Release 15.2M&T
- Cisco IOS Carrier Ethernet Command Reference
- IP Addressing: ARP Configuration Guide, Cisco IOS Release 15M&T
- Cisco IOS LAN Switching Command Reference
- Layer 2 Switching Software Configuration Guide for IE 2000U and Connected Grid Switches

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

Configuring the Switch Alarms

This chapter describes how to configure alarms on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*. This chapter includes the following sections:

Note For complete syntax and usage information for the commands used in this chapter, see the switch command reference listed in the "Related Documents" section on page 5-14.

Note For information about the alarm input and output ports, see the *Cisco IE 2000U Switch Hardware Installation Guide*.

Information About Switch Alarms

The switch software monitors switch conditions on a per-port or a switch basis. If the conditions present on the switch or a port do not match the set parameters, the switch software triggers an alarm or a system message. By default, the switch software sends the system messages to a system message logging facility, or a *syslog* facility. You can also configure the switch to send Simple Network Management Protocol (SNMP) traps to an SNMP server. You can configure the switch to trigger an external alarm device by using the alarm relay. For more information on how to configure the alarms, see the "Configuring Switch Alarms" section on page 5-7.

This section includes the following topics:

Global Status Monitoring Alarms

The switch processes alarms related power supply conditions, referred to as global or facility alarms.

Table 5-1 Switch Global Status Monitoring Alarms

Alarm	Description
Power supply alarm	The switch monitors dual power supply levels. If there are two power supplies installed in the switch, an alarm triggers if a power supply fails. The alarm is automatically cleared when both power supplies are working. You can configure the power supply alarm to be connected to the hardware relays. For more information, see the "Configuring the Power Supply Alarms" section on page 5-7.

FCS Error Hysteresis Threshold

The Ethernet standard calls for a maximum bit error rate of 10^{-8}. On the switch, the bit error rate range is from 10^{-6} to 10^{-11}. The bit error rate input to the switch is a positive exponent. If you want to configure the bit error rate of 10^{-9}, enter the value 9 for the exponent. By default, the FCS bit error rate is 10^{-8}.

You can set the FCS error hysteresis threshold to prevent the toggle of the alarm when the actual bit error rate fluctuates near the configured rate. The hysteresis threshold is defined as the ratio between the alarm clear threshold to the alarm set threshold, expressed as a percentage value.

For example, if the FCS bit error rate alarm value is configured to 10^{-8}, that value is the alarm set threshold. To set the alarm clear threshold at $5*10^{-10}$, the hysteresis, value *h*, is determined as follows:

h = alarm clear threshold / alarm set threshold

$h = 5*10^{-10} / 10^{-8} = 5*10^{-2} = 0.05 = 5$ percent

The FCS hysteresis threshold is applied to all ports on the switch. The allowable range is from 1 to 10 percent. The default value is 10 percent. See the "Configuring the FCS Bit Error Rate Alarm" section on page 5-8 for more information.

Port Status Monitoring Alarms

The switch can also monitor the status of the Ethernet ports and generate alarm messages based on the alarms listed in Table 5-2. To save user time and effort, it supports changeable alarm configurations by using alarm profiles. You can create a number of profiles and assign one of these profiles to each Ethernet port.

Alarm profiles provide a mechanism for you to enable or disable alarm conditions for a port and associate the alarm conditions with one or both alarm relays. You can also use alarm profiles to set alarm conditions to send alarm traps to an SNMP server and system messages to a syslog server. The alarm profile *defaultPort* is applied to all interfaces in the factory configuration (by default).

Note You can associate multiple alarms to one relay or one alarm to both relays.

Table 5-2 lists the port status monitoring alarms and their descriptions and functions. Each fault condition is assigned a severity level based on the Cisco IOS System Error Message Severity Level.

Table 5-2 Switch Port Status Monitoring Alarms

Alarm	Description
Link Fault alarm	The switch generates a link fault alarm when problems with a port physical layer cause unreliable data transmission. A typical link fault condition is loss of signal or clock. The link fault alarm is cleared automatically when the link fault condition is cleared. The severity for this alarm is *error condition*, level 3.
Port not Forwarding alarm	The switch generates a port not forwarding alarm when a port is not forwarding packets. This alarm is cleared automatically when the port begins to forward packets. The severity for this alarm is *warning*, level 4.
Port not Operating alarm	The switch generates a port not operating alarm when a port fails during the startup self-test. When triggered, the port not-operating alarm is only cleared when the switch is restarted and the port is operational. The severity for this alarm is *error condition*, level 3.
FCS Bit Error Rate alarm	The switch generates an FCS bit error rate alarm when the actual FCS bit error rate is close to the configured rate. You can set the FCS bit error rate by using the interface configuration CLI for each of the ports. See the "Configuring the FCS Bit Error Rate Alarm" section on page 5-8 for more information. The severity for this alarm is *error condition*, level 3.

Triggering Alarm Options

The switch supports these methods for triggering alarms:

- Configurable Relay

  The switch is equipped with one independent alarm relay that can be triggered by alarms for global and port status conditions. You can configure the relay to send a fault signal to an external alarm device, such as a bell, light, or other signaling device. You can associate any alarm condition with the alarm relay. Each fault condition is assigned a severity level based on the Cisco IOS System Error Message Severity Level.

  See the "Configuring Switch Alarms" section on page 5-7 for more information on configuring the relay.

- SNMP Traps

  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 management information base (MIB).

  The **snmp-server enable traps** command can be changed so that the user can send alarm traps to an SNMP server. You can use alarm profiles to set environmental or port status alarm conditions to send SNMP alarm traps. See the "Enabling SNMP Traps" section on page 5-12 for more information.

- Syslog Messages

You can use alarm profiles to send system messages to a syslog server. See the "Configuring Switch Alarms" section on page 5-7 for more information.

Prerequisites

Review the "Information About Switch Alarms" section on page 5-1.

Guidelines and Limitations

The **snmp-server enable traps alarms** command is used in conjunction with the snmp-server host command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send notifications, you must configure at least one **snmp-server host** command. See Chapter 14, "Configuring SNMP".

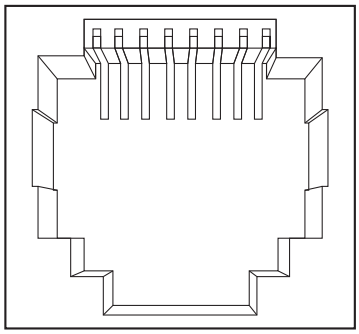
Default Settings

	Alarm	Default Setting
Global	Power supply alarm	Enabled in switch single power mode. No alarm. In dual-power supply mode, the default alarm notification is a system message to the console.
Port	Link fault alarm	Disabled on all interfaces.
	Port not forwarding alarm	Disabled on all interfaces.
	Port not operating alarm	Enabled on all interfaces.
	FCS bit error rate alarm	Disabled on all interfaces.

Configuring External 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 5-1 Alarm Port Pinouts

Pin	Alarm connection	1 2 3 4 5 6 7 8
1	Alarm 1 input	
2	Alarm 2 input	
3	Normally closed	
4	Alarm 3 input	
5	Alarm 4 input	
6	Normally open	
7	Alarm output common	
8	Alarm input common	

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 IE 2000U Switch 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**.

BEFORE YOU BEGIN

Review the "Global Status Monitoring Alarms" section on page 5-2.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**alarm contact** *contact-number* **description** *string*	(Optional) Configure a description for the alarm contact number. • The *contact-number* is from 1 to 4. • The description string is up to 80 alphanumeric characters in length and is included in any generated system messages.

	Command	Purpose
Step 3	**alarm contact** {*contact-number* | **all**} {**severity** {**critical** | **major** | **minor**} | **trigger** {**closed** | **open**}}	Configure the trigger and severity for an alarm contact number or for all contact numbers. • Enter a contact number (1 to 4) or specify that you are configuring **all** alarms. See Figure 5-1 for the alarm contact pinouts. • For **severity**, enter **critical**, **major**, or **minor**. If you do not configure a severity, the default is **minor**. • For **trigger**, enter **open** or **closed**. If you do not configure a trigger, the alarm is triggered when the circuit is **closed**.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show env alarm-contact**	Show the configured alarm contacts.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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 listed in the "Related Documents" section on page 5-14.

Note The switch supports the CISCO-ENTITY-ALARM-MIB for these alarms.

EXAMPLE

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
```

Configuring Switch Alarms

This section includes the following topics:

Configuring the Power Supply Alarms

The presence of power supplies is dynamically detected. Use the **show env power** command in privileged EXEC or user EXEC mode to display power information for the switch.

Use the **alarm facility power-supply rps** global configuration command to associate the switch redundant power supply (RPS) alarm to the relay. You can also configure all alarms and traps associated with the RPS to be sent to syslog and the SNMP server.

BEFORE YOU BEGIN

Before you can use the **notifies** command to send alarm traps to an SNMP server, you must first set up the SNMP server by using the **snmp-server enable traps alarms** global configuration command. See the "Enabling SNMP Traps" section on page 5-12.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**alarm facility power-supply rps relay major**	Associate the RPS alarm to the relay.
Step 3	**alarm facility power-supply rps notifies**	Send RPS alarm traps to an SNMP server.
Step 4	**alarm facility power-supply rps syslog**	Send RPS alarm traps to a syslog server.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show alarm settings**	Verify the configuration.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable sending the alarm to a relay, to syslog, or to an SNMP server, use the **no alarm facility power-supply rps relay**, **no alarm facility power-supply rps notifies**, or **no alarm facility power-supply rps syslog** global configuration commands.

EXAMPLE

This example sets the RPS monitoring alarm to the major relay:

```
Switch(config) # alarm facility power-supply rps relay major
```

Configuring the FCS Bit Error Rate Alarm

Setting the FCS Error Threshold

The switch generates an FCS bit error rate alarm when the actual rate is close to the configured rate. Use the **fcs-threshold** interface configuration command to set the FCS error threshold.

BEFORE YOU BEGIN

Review the "FCS Error Hysteresis Threshold" section on page 5-2.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter the interface to be configured, and enter interface configuration mode.
Step 3	**fcs-threshold** ***value***	Set the FCS bit error rate. For *value*, the range is 6 to 11 to set a maximum bit error rate of 10^{-6} to 10^{-11}. By default, the FCS bit error rate is 10^{-8}.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show fcs-threshold**	Verify the setting.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no fcs-threshold** interface configuration command to return to the default FCS threshold value.

EXAMPLE

This example shows how to set the FCS bit error rate for a port to 10^{-10}:

```
Switch# configure terminal
Switch(config)# interface fastethernet1/1
Switch(config-if) # fcs-threshold 10
```

Setting the FCS Error Hysteresis Threshold

The hysteresis setting prevents the toggle of an alarm when the actual bit error rate fluctuates near the configured rate. Use the **alarm facility fcs-hysteresis** global configuration command to set the FCS error hysteresis threshold.

Note The FCS hysteresis threshold is applied to all ports of a switch.

BEFORE YOU BEGIN

Review the "FCS Error Hysteresis Threshold" section on page 5-2.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**alarm facility fcs-hysteresis** *percentage*	Set the hysteresis percentage for the switch. For *percentage*, the range is 1 to 10. The default value is 10 percent.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running config**	Verify the configuration.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no alarm facility fcs-hysteresis** command to set the FCS error hysteresis threshold to its default value.

Note The **show running config** command displays any FCS error hysteresis that is not the default value.

EXAMPLE

This example shows how to set the FCS error hysteresis at 5 percent:

```
Switch(config)# alarm facility fcs-hysteresis 5
```

Configuring Alarm Profiles

Creating or Modifying an Alarm Profile

You can use the **alarm profile** global configuration command to create an alarm profile or to modify an existing profile. When you create a new alarm profile, none of the alarms are enabled.

Note The only alarm enabled in the *defaultPort* profile is the Port not operating alarm.

BEFORE YOU BEGIN

Before you use the **notifies** command to send alarm traps to an SNMP server, you must first set up the SNMP server by using the **snmp-server enable traps alarms** global configuration command. See the "Enabling SNMP Traps" section on page 5-12.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**alarm profile** ***name***	Create the new profile or identify an existing profile, and enter alarm profile configuration mode.
Step 3	**alarm** *alarm-id*	Add or modify alarm parameters for a specific alarm (see Table 5-3). The values are 1 to 4. You can enter more than one alarm ID separated by a space.
Step 4	**notifies** *alarm-id*	(Optional) Configure the alarm to send an SNMP trap to an SNMP server.
Step 5	**relay-major** *alarm-id*	(Optional) Configure the alarm to send an alarm trap to the relay.
Step 6	**syslog** *alarm-id*	(Optional) Configure the alarm to send an alarm trap to a syslog server.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show alarm profile** ***name***	Verify the configuration.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To delete an alarm profile, use the **no alarm profile** *name* global configuration command.

Table 5-3 lists the *alarmList* IDs and their corresponding alarm definitions. For a description of these alarms, see the "Port Status Monitoring Alarms" section on page 5-2.

Table 5-3 AlarmList ID Number Alarm Descriptions

AlarmList ID	Alarm Description
1	Link fault
2	Port not forwarding
3	Port not operating
4	FCS bit error rate exceeds threshold

EXAMPLE

This example creates or modifies the alarm profile *fastE* for the Fast Ethernet port with link-down (*alarmList* ID 3) alarm enabled. The link-down alarm is connected to the major relay. This alarm also send notifications to an SNMP server and sends system messages to a syslog server.

```
Switch(config)# alarm profile fastE
Switch(config-alarm-prof)# alarm 3
Switch(config-alarm-prof)# relay major 3
Switch(config-alarm-prof)# notifies 3
Switch(config-alarm-prof)# syslog 3
```

Attaching an Alarm Profile to a Specific Port

In interface configuration mode, you can use the **alarm-profile** command to attach an alarm profile to a specific port.

BEFORE YOU BEGIN

Review the "Port Status Monitoring Alarms" section on page 5-2.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *port interface*	Enter the number of the switch port to be configured, and the switch enters interface configuration mode.
Step 3	**alarm-profile** *name*	Attach the specified profile to the interface.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show alarm profile**	Verify the configuration.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To detach an alarm profile from a specific port, use the **no alarm-profile** *name* interface configuration command.

EXAMPLE

This example attaches an alarm profile named *fastE* to a port:

```
Switch(config)# interface fastethernet 1/2
Switch(config-if)# alarm profile fastE
```

This example detaches an alarm profile named *fastE* from a port:

```
Switch(config)# interface fastethernet 1/2
Switch(config-if)# no alarm profile fastE
```

Enabling SNMP Traps

Use the **snmp-server enable traps alarms** global configuration command to enable the switch to send *alarm* traps.

BEFORE YOU BEGIN

The **snmp-server enable traps alarms** command is used in conjunction with the snmp-server host command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send notifications, you must configure at least one **snmp-server host** command.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**snmp-server enable traps alarms**	Enable the switch to send SNMP traps.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show alarm settings**	Verify the configuration.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

```
Switch(config)# snmp-server enable traps alarms
```

Verifying Configuration

Command	Purpose
show alarm description port	Displays an alarm number and its text description.
show alarm profile [*name*]	Displays all alarm profiles in the system or a specified profile.
show alarm settings	Displays all global alarm settings on the switch.
show env {all | power | temperature}	Displays the status of environmental facilities on the switch.
show facility-alarm status [critical | info | major]	Displays generated alarms on the switch.

Configuration Example

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
```

This example sets the RPS monitoring alarm to the major relay:

```
Switch(config) # alarm facility power-supply rps relay major
```

This example shows how to set the FCS bit error rate for a port to 10^{-10}:

```
Switch# configure terminal
Switch(config)# interface fastethernet1/1
Switch(config-if) # fcs-threshold 10
```

This example shows how to set the FCS error hysteresis at 5 percent:

```
Switch(config)# alarm facility fcs-hysteresis 5
```

This example creates or modifies the alarm profile *fastE* for the Fast Ethernet port with link-down (*alarmList* ID 3) alarm enabled. The link-down alarm is connected to the major relay. This alarm also send notifications to an SNMP server and sends system messages to a syslog server.

```
Switch(config)# alarm profile fastE
Switch(config-alarm-prof)# alarm 3
Switch(config-alarm-prof)# relay major 3
Switch(config-alarm-prof)# notifies 3
Switch(config-alarm-prof)# syslog 3
```

This example attaches an alarm profile named *fastE* to a port:

```
Switch(config)# interface fastethernet 1/2
Switch(config-if)# alarm profile fastE
```

This example detaches an alarm profile named *fastE* from a port:

```
Switch(config)# interface fastethernet 1/2
Switch(config-if)# no alarm profile fastE
```

Related Documents

- Cisco IOS Master Command List, All Releases
- Cisco IE 2000U Switch Hardware Installation Guide

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520	Cisco IOS Release 12.2(53)EX

Configuring SDM Templates

This chapter describes how to configure the Switch Database Management (SDM) templates on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*. SDM template configuration is supported in both IP Services and LAN Base images.

Note For complete syntax and usage information for the commands used in this chapter, see the command reference listed in the "Related Documents" section on page 6-7.

This chapter includes the following sections:

Information About the SDM Templates

If the switch is running the IP services image, you can use SDM templates 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 for IP Version 4 (IPv4) and select the default template to balance system resources or select the layer-2 template to support only Layer 2 features in hardware.

- Layer-2—The layer-2 template maximizes system resources for Layer 2 functionality and does not support routing. You should use this template when the switch is being used for Layer 2 forwarding. When you select the layer-2 template on a switch running the IP services image, any routing is done through software, which overloads the CPU and severely degrades routing performance.

- Default—The default template gives balance to all functions: Layer 2 and Layer 3 (routing). This template is available on switches running either the IP Services or LAN Base image. If you do not use the default template with IP Services image and with routing enabled on the switch (that is, you use the layer-2 template instead), any routing is done through software, which overloads the CPU and severely degrades routing performance.

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

Table 6-1 shows the approximate number of each resource supported in each of the two IPv4 templates. The values in the template are based on eight routed interfaces and approximately 1024 VLANs and represent the approximate hardware boundaries set when a template is selected. If a section of a hardware resource is full, all processing overflow is sent to the CPU, seriously impacting switch performance.

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

Resource	Layer-2	Default
Unicast MAC addresses	8 K	5 K
IPv4 IGMP groups + multicast routes (default only)	–	1 K
IP v4 IGMP groups (layer-2 only)	1 K	–
IPv4 multicast routes (layer-2 only)	0	–
IPv4 IGMP groups and multicast routes	1 K	–
IPv4 unicast routes	0	9 K
• Directly connected IPv4 hosts	–	5 K
• Indirect IPv4 routes	–	4 K
IPv4 policy-based routing ACEs[1]	0	0.5 K
IPv4 or MAC QoS[2] ACEs	0.5 K	0.5 K
IPv4 or MAC security ACEs	1 K	1 K

1. ACEs = Access control entries.
2. QoS = Quality of service.

Dual IPv4 and IPv6 SDM Templates

You can select SDM templates to support IP Version 6 (IPv6). For more information about IPv6 and how to configure IPv6 routing, see the "Configuring IPv6 Unicast Routing" chapter in the *Unicast Routing Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*. For information about configuring IPv6 ACLs, see the "Configuring IPv6 ACLs" chapter in the *Security Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*.

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

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

These SDM templates support IPv4 and IPv6 environments:

- Dual IPv4 and IPv6 default template—supports Layer 2, multicast, routing, QoS, and ACLs for IPv4; and Layer 2, routing, and ACLs for IPv6 on the switch.

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

This software release does not support IPv6 multicast routing, IPv6 QoS, or IPv6 Multicast Listener Discovery (MLD) snooping.

Note An IPv4 route requires only one TCAM entry. Because of the hardware compression scheme used for IPv6, an IPv6 route can take more than one TCAM entry, reducing the number of entries forwarded in hardware.

Table 6-2 defines the approximate feature resources allocated by each dual template. Template estimations are based on a switch with 8 routed interfaces and approximately 1000 VLANs.

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

Resource	IPv4-and-IPv6 Default	IPv4-and-IPv6 Routing	IPv4-and-IPv6 VLAN
Unicast MAC addresses	2 K	1.5 K	8 K
IPv4 IGMP groups and multicast routes	1 K	1K	1 K
Total IPv4 unicast routes:	3 K	2.75 K	0
• Directly connected IPv4 hosts	2 K	1.5 K	0
• Indirect IPv4 routes	1 K	1.25 K	0
IPv6 multicast groups	1 K	1 K	1 K
Total IPv6 unicast routes:	3 K	2.75 K	0
• Directly connected IPv6 addresses	2 K	1.5 K	0
• Indirect IPv6 unicast routes	1 K	1.25 K	0
IPv4 policy-based routing ACEs	0	0.25 K	0
IPv4 or MAC QoS ACEs (total)	0.75 K	0.75 K	0.75 K
IPv4 or MAC security ACEs (total)	1 K	0.5 K	1K
IPv6 policy-based routing ACEs[1]	0	0.25 K	0
IPv6 QoS ACEs	0.5 K	0.5 K	0.5 K
IPv6 security ACEs	0.5 K	0.5 K	0.5 K

1. IPv6 policy-based routing is not supported.

Prerequisites

Determine whether routing is enabled on the switch and whether you have both IPv6 and IPv4 traffic on the network.

Guidelines and Limitations

Follow these guidelines when selecting and configuring SDM templates:

- You must reload the switch for the configuration to take effect.
- If you are using the switch for Layer 2 features only, select the layer-2 template.
- Do not use the default template if you do not have routing enabled on your switch. The **sdm prefer default** global configuration command prevents other features from using the memory allocated to unicast routing in the routing template.
- You should use the default template when you plan to enable routing on the switch. If you do not use the default template when routing is enabled, routing is done through software, which overloads the CPU and severely degrades routing performance.
- If you try to configure IPv6 features without first selecting a dual IPv4 and IPv6 template, a warning message is generated.
- Using the dual stack templates results in less TCAM capacity allowed for each resource, so do not use if you plan to forward only IPv4 traffic.
- In the event that you are swapping your SD flash card from a failed unit to a replacement unit and you are not using the default template, you need to re-configure the preferred SDM template and then reload the switch for the selected template to take effect.

Note For details on how to replace (swap) the SD flash card, see the "Switch Installation" chapter within the *Cisco IE 2000U Switch Hardware Installation Guide*.

Default Settings

The default template for a switch running either the IP services or LAN Base image is the default template.

Configuring the Switch SDM Template

Follow this procedure to use the SDM template to select a template on a switch running the IP services image.

BEFORE YOU BEGIN

Review the "Guidelines and Limitations" section on page 6-4.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**sdm prefer** {**default** | **dual-ipv4-and-ipv6** {**default** | **routing** | **vlan**} | **layer-2**}	Specify the SDM template to be used on the switch: The keywords have these meanings: • **default**—Balance all functions. • **dual-ipv4-and-ipv6**—Select a template that supports both IPv4 and IPv6 routing. – **default**—Balance IPv4 and IPv6 Layer 2 and Layer 3 functionality. – **routing**—Provide maximum usage for IPv4 and IPv6 routing, including IPv4 policy-based routing. – **vlan**—Provide maximum usage for IPv4 and IPv6 VLANs. • **layer-2**—Support Layer 2 functionality and do not support routing on the switch.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**reload**	Reload the operating system.

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

EXAMPLE

This is an example of an output display when you have changed the template to the layer-2 template and have not reloaded the switch:

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

  number of unicast mac addresses:                  5K
  number of IPv4 IGMP groups + multicast routes:    1K
  number of IPv4 unicast routes:                    9K
    number of directly-connected IPv4 hosts:        5K
    number of indirect IPv4 routes:                 4K
  number of IPv4 policy based routing aces:         0.5K
  number of IPv4/MAC qos aces:                      0.5K
  number of IPv4/MAC security aces:                 1K
On next reload, template will be "layer-2" template.
```

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

This example shows how to configure a switch with the layer-2 template:

```
Switch(config)# sdm prefer layer-2
Switch(config)# end
Switch# reload
Proceed with reload? [confirm]
```

Verifying Configuration

Use the **show sdm prefer** privileged EXEC command with no parameters to display the active template. Use the **show sdm prefer [default | dual-ipv4-and-ipv6 {default | routing | vlan} | layer-2]** privileged EXEC command to display the resource numbers supported by the specified template.

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

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

  number of unicast mac addresses:                  5K
  number of IPv4 IGMP groups + multicast routes:    1K
  number of IPv4 unicast routes:                    9K
    number of directly-connected IPv4 hosts:        5K
    number of indirect IPv4 routes:                 4K
  number of IPv4 policy based routing aces:         0.5K
  number of IPv4/MAC qos aces:                      0.5K
  number of IPv4/MAC security aces:                 1K
```

This is an example of output from the **show sdm prefer layer-2** command:

```
Switch# show sdm prefer layer-2
"layer-2" template:
 The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:                  8K
  number of IPv4 IGMP groups:                       1K
  number of IPv4 multicast routes:                  0
  number of IPv4 unicast routes:                    0
  number of IPv4 policy based routing aces:         0
  number of IPv4/MAC qos aces:                      0.5K
  number of IPv4/MAC security aces:                 1K
```

This is an example of output from the **show sdm prefer dual-ipv4-and-ipv6 routing** command:

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

  number of unicast mac addresses:                  1.5K
  number of IPv4 IGMP groups + multicast routes:    1K
  number of IPv4 unicast routes:                    2.75K
    number of directly-connected IPv4 hosts:        1.5K
    number of indirect IPv4 routes:                 1.25K
  number of IPv6 multicast groups:                  1.125k
```

```
  number of directly-connected IPv6 addresses:      1.5K
  number of indirect IPv6 unicast routes:           1.25K
  number of IPv4 policy based routing aces:         0.25K
  number of IPv4/MAC qos aces:                      0.75K
  number of IPv4/MAC security aces:                 0.5K
  number of IPv6 policy based routing aces:         0.25K
  number of IPv6 qos aces:                          0.5K
  number of IPv6 security aces:                     0.5K
```

Configuration Example

This is an example of an output display when you have changed the template to the layer-2 template and have not reloaded the switch:

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

  number of unicast mac addresses:                  5K
  number of IPv4 IGMP groups + multicast routes:    1K
  number of IPv4 unicast routes:                    9K
    number of directly-connected IPv4 hosts:        5K
    number of indirect IPv4 routes:                 4K
  number of IPv4 policy based routing aces:         0.5K
  number of IPv4/MAC qos aces:                      0.5K
  number of IPv4/MAC security aces:                 1K
On next reload, template will be "layer-2" template.
```

This example shows how to configure a switch with the layer-2 template:

```
Switch(config)# sdm prefer layer-2
Switch(config)# end
Switch# reload
Proceed with reload? [confirm]
```

Related Documents

- Cisco IOS Master Command List, All Releases
- Unicast Routing Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches
- Security Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches
- Cisco IE 2000U Switch Hardware Installation Guide

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

Configuring Smartports Macros

This chapter describes how to configure Smartports macros on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*. This chapter includes the following sections:

Information About Smartports Macros

Smartports macros provide a convenient way to save and share common configurations. You can use Smartports macros to enable features and settings based on the location of a switch in the network and for mass configuration deployments across the network.

Each Smartports macro is a set of CLI commands. The switch software has a set of default macros. You can also create your own macros. Smartports macros do not contain new CLI commands; they are simply a group of existing CLI commands.

A macro can be user defined or system default (which cannot be edited by user).

Prerequisites

You must be familiar with the switch CLI commands.

Guidelines and Limitations

- You can apply a macro globally or to a specific switch interface.

- 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 you apply a macro to an interface, the CLI commands within the macro are configured on the interface. The existing interface configurations are not lost.

  The new commands are added to the interface and are saved in the running configuration file. This is helpful when applying an incremental configuration
- If a command fails because of a syntax or a configuration error, the macro continues to apply the remaining 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.
- 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.
- 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.
- Some CLI commands are specific to certain interface types. If you apply a macro to an interface that does not accept the configuration, the macro fails the syntax or the configuration check, and the switch returns 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.

Default Settings

There are no Smartports macros enabled on the switch. The system default macros are listed in Table 7-1.

Table 7-1 Default Smartports Macros

Macro Name[1]	Description
Global Configuration Macros	
cisco-cg-global	Use this global configuration macro to configure the switch settings for the industrial Ethernet environment. This macro is automatically applied when you use Express Setup to initially configure the switch. **Note** You must first apply the **cisco-cg-global** macro for the interface configuration macros to work properly.
cisco-cg-password	Use this global configuration macro to configure the password settings for the switch.
no-cisco-cg-password	Use the **no** form of this global configuration macro to delete the macro from the switch.
cisco-sniffer	Use this global configuration macro to configure SPAN functionality to analyze traffic on another port of the switch.
no-cisco-sniffer	Use the **no** form of this global configuration macro to delete the macro from the interface.
Interface Configuration Macros	
cisco-cg-hmi	Use this interface configuration macro for increased network security and reliability when connecting a desktop device, such as a PC, to a switch port. This macro is optimized for utility deployments.
no-cisco-cg-hmi	Use the **no** form of this interface configuration macro to delete the macro from the switch.
cisco-cg-ied	Use this interface configuration macro when connecting the switch to an IED.
no-cisco-cg-ied	Use the **no** form of this interface configuration macro to delete the macro from the switch.
cisco-cg-router	Use this interface configuration macro when connecting the switch and a WAN router. This macro is optimized for utility deployments.
no-cisco-cg-router	Use the **no** form of this interface configuration macro to delete the macro from the switch.
cisco-cg-switch	Use this interface configuration macro when connecting a ring of switches. This macro is optimized for utility deployments.
no-cisco-cg-switch	Use the **no** form of this interface configuration macro to delete the macro from the switch.
cisco-cg-wireless	Use this interface configuration macro when connecting the switch and a wireless access point. This macro is optimized for utility deployments.
no-cisco-cg-wireless	Use the **no** form of this interface configuration macro to delete the macro from the switch.
cisco-desktop	Use this interface configuration macro for increased network security and reliability when connecting a desktop device, such as a PC, to a switch port. This macro is optimized for utility deployments.
no-cisco-desktop	Use the **no** form of this interface configuration macro to delete the macro from the interface.

1. Cisco-default Smartports macros vary, depending on the software version running on your switch.

Configuring Smartports Macros

This section includes the following topics:

Creating Smartports Macros

BEFORE YOU BEGIN

Review the "Guidelines and Limitations" section on page 7-1.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**macro name** *macro-name*	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.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show parser macro name** *macro-name*	Verify that the macro was created.

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.

EXAMPLE

This example shows how to create a macro that defines the switchport access VLAN and the number of secure MAC addresses and also includes two help string keywords by using **# macro keywords**:

```
Switch(config)# macro name test
switchport access vlan $VLANID
switchport port-security maximum $MAX
#macro keywords $VLANID $MAX
@
```

Applying Smartports Macros

BEFORE YOU BEGIN

Review the "Guidelines and Limitations" section on page 7-1.

DETAILED STEPS

	Command	Purpose
Step 1	**show parser macro**	Display the Cisco-default Smartports macros embedded in the switch software.
Step 2	**show parser macro name** *macro-name*	Display the specific macro that you want to apply.
Step 3	**configure terminal**	Enter global configuration mode.
Step 4	**macro global** {**apply** | **trace**} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]	Apply each individual command defined in the macro to the switch by entering **macro global apply** *macro-name*. Specify **macro global trace** *macro-name* to apply and to debug a macro to find any syntax or configuration errors. Append the macro with the required values by using the **parameter** *value* keywords. Keywords that begin with **$** require a unique parameter value. You can use the **macro global apply** *macro-name* **?** command to display a list of any required values for the macro. If you apply a macro without entering the keyword values, the commands are invalid and are not applied. (Optional) Specify unique parameter values that are specific to the switch. You can enter up to three keyword-value pairs. Parameter keyword matching is case sensitive. The corresponding value replaces all matching occurrences of the keyword.
Step 5	**interface** *interface-id*	(Optional) Enter interface configuration mode, and specify the interface on which to apply the macro.
Step 6	**default interface** *interface-id*	(Optional) Clear all configuration from the specified interface.

	Command	Purpose
Step 7	**macro** {**apply** | **trace**} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]	Apply each individual command defined in the macro to the port by entering **macro apply** *macro-name*. Specify **macro trace** *macro-name* to apply and to debug a macro to find any syntax or configuration errors. Append the macro with the required values by using the **parameter** *value* keywords. Keywords that begin with **$** require a unique parameter value. You can use the **macro apply** *macro-name* **?** command to display a list of any required values for the macro. If you apply a macro without entering the keyword values, the commands are invalid and are not applied. (Optional) Specify unique parameter values that are specific to the switch. You can enter up to three keyword-value pairs. Parameter keyword matching is case sensitive. The corresponding value replaces all matching occurrences of the keyword.
Step 8	**end**	Return to privileged EXEC mode.
Step 9	**show running-config interface** *interface-id*	Verify that the macro is applied to an interface.
Step 10	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

You can delete the **cisco-cg-password** and **cisco-sniffer** global macros on a switch by entering the **no** version of each command in the macro. The **cisco-cg-global** global macro does not have a **no** version. You can delete a macro-applied configuration on a port by entering the **default interface** *interface-id* interface configuration command.

EXAMPLE

This example shows how to display the **cisco-desktop** macro and how to set the access VLAN ID to 25 on an interface:

```
Switch# show parser macro name cisco-desktop
Macro name : cisco-desktop
Macro type : default interface
# Macro keywords $access_vlan
# macro description cisco-desktop
switchport access vlan $access_vlan
switchport port-security
switchport port-security maximum 1
switchport port-security aging time 2
switchport port-security violation restrict
switchport port-security aging type inactivity
port-type nni
spanning-tree portfast
spanning-tree bpduguard enable

Switch# configure terminal
Switch(config-if)# interface fastethernet 0/2
Switch(config-if)# macro trace cisco-desktop $access_vlan 25
Applying command... 'macro description cisco-desktop'
Applying command... 'switchport access vlan 25'
Applying command... 'switchport port-security'
```

```
Applying command... 'switchport port-security maximum 1'
Applying command... 'switchport port-security aging time 2'
Applying command... 'switchport port-security violation restrict'
Applying command... 'switchport port-security aging type inactivity'
Applying command... 'port-type nni'
Applying command... 'spanning-tree portfast'
```

Verifying Configuration

Command	Purpose
show parser macro	Displays all Smartports macros.
show parser macro name *macro-name*	Displays a specific Smartports macro.
show parser macro brief	Displays the Smartports macro names.
show parser macro description [**interface** *interface-id*]	Displays the Smartports macro description for all interfaces or for a specified interface.

Configuration Example

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
@
```

This example shows how to display the **cisco-desktop** macro and how to set the access VLAN ID to 25 on an interface:

```
Switch# show parser macro name cisco-desktop
Macro name : cisco-desktop
Macro type : default interface
# Macro keywords $access_vlan
# macro description cisco-desktop
switchport access vlan $access_vlan
switchport port-security
switchport port-security maximum 1
switchport port-security aging time 2
switchport port-security violation restrict
switchport port-security aging type inactivity
port-type nni
spanning-tree portfast
spanning-tree bpduguard enable

Switch# configure terminal
Switch(config-if)# interface fastethernet 0/2
Switch(config-if)# macro trace cisco-desktop $access_vlan 25
Applying command... 'macro description cisco-desktop'
Applying command... 'switchport access vlan 25'
Applying command... 'switchport port-security'
Applying command... 'switchport port-security maximum 1'
Applying command... 'switchport port-security aging time 2'
Applying command... 'switchport port-security violation restrict'
```

```
Applying command... 'switchport port-security aging type inactivity'
Applying command... 'port-type nni'
Applying command... 'spanning-tree portfast'
```

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

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 Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*.

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 8-10.

This chapter includes the following sections:

Information About LLDP and LLDP-MED

This section includes the following topics:

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.

LLDP is enabled by default on network node interfaces (NNIs). It is disabled on enhanced network interfaces (ENIs), but you can enable it. LLDP is not supported on user network interfaces (UNIs).

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)

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.

Prerequisites

- Type-Length-Value (TLV) types 0 through 127
- To support LLDP-MED, the following organizationally specific TLVs must be implemented:
  - Extended Power-via-Media Dependent Interface (MDI)
  - Inventory
  - LLDP-MED Capabilities
  - MAC/PHY Configuration Status
  - Network Policy
  - Port VLAN ID

Guidelines and Limitations

- Use of LLDP is limited to 802.1 media types such as Ethernet, Token Ring, and Fiber Distributed Data Interface (FDDI) networks.
- The maximum number of neighbor entries per chassis is limited on MED-capable network connectivity devices.

Default Settings

Feature	Default Setting
LLDP global state	Disabled
LLDP holdtime (before discarding)	120 seconds
LLDP timer (packet update frequency)	30 seconds
LLDP reinitialization delay	2 seconds
LLDP tlv-select	Disabled to send and receive all TLVs
LLDP interface state	Disabled
LLDP receive	Enabled on network node interfaces (NNIs) Disabled on enhanced network interfaces (ENIs) Not supported on user network interfaces (UNIs)
LLDP transmit	Enabled on NNIs Disabled on ENIs Not supported on UNIs
LLDP med-tlv-select	Disabled to send all LLDP-MED TLVs

Configuring LLDP and LLDP-MED

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.

BEFORE YOU BEGIN

Review the "Information About LLDP and LLDP-MED" section on page 8-1.

DETAILED STEPS

Note Steps 2 through 5 are all optional and can be performed in any order.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**lldp 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 0 to 65535 seconds; the default is 120 seconds.
Step 3	**lldp reinit**	(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.
Step 4	**lldp timer** *seconds*	(Optional) Set the transmission frequency of LLDP updates in seconds. The range is 5 to 65534 seconds; the default is 30 seconds.
Step 5ll	**lldp tlv-select**	(Optional) Specify the LLDP TLVs to send or receive.
Step 6	**lldp med-tlv-select**	(Optional) Specify the LLDP-MED TLVs to send or receive.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of each of the LLDP commands to return to the default setting.

EXAMPLE

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
```

Disabling and Enabling LLDP Globally

LLDP is disabled globally by default and is enabled on NNIs. It is disabled by default on ENIs, but can be enabled per interface. LLDP is not supported on UNIs.

Disabling LLDP

BEFORE YOU BEGIN

Review the "Information About LLDP and LLDP-MED" section on page 8-1.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no lldp run**	Disable LLDP.
Step 3	**end**	Return to privileged EXEC mode.

EXAMPLE

This example shows how to globally disable LLDP:

```
Switch# configure terminal
Switch(config)# no lldp run
Switch(config)# end
```

Enabling LLDP

BEFORE YOU BEGIN

Review the "Information About LLDP and LLDP-MED" section on page 8-1.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.

	Command	Purpose
Step 2	**lldp run**	Enable LLDP.
Step 3	**end**	Return to privileged EXEC mode.

EXAMPLE

This example shows how to globally enable LLDP:

```
Switch# configure terminal
Switch(config)# lldp run
Switch(config)# end
```

Disabling and Enabling LLDP on an Interface

LLDP is disabled by default on all NNIs to send and to receive LLDP information. It is disabled by default on ENIs, but it can be enabled by entering the **lldp transmit** and **lldp receive** interface configuration commands. LLDP is not supported on UNIs.

Note If the interface is configured as a tunnel port, LLDP is automatically disabled.

Disabling LLDP on an Interface

BEFORE YOU BEGIN

Review the "Information About LLDP and LLDP-MED" section on page 8-1.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface on which you are disabling LLDP, and enter interface configuration mode. The interface must be an NNI or ENI for the **lldp** commands to be available.
Step 3	**no lldp transmit**	No LLDP packets are sent on the interface.
Step 4	**no lldp receive**	No LLDP packets are received on the interface.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

This example shows how to disable LLDP on an interface:

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet1/0/1
Switch(config-if)# no lldp transmit
Switch(config-if)# no lldp receive
Switch(config-if)# end
```

Enabling LLDP on an Interface

BEFORE YOU BEGIN

Review the "Information About LLDP and LLDP-MED" section on page 8-1.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface on which you are enabling LLDP, and enter interface configuration mode. LLDP is supported only on NNIs and ENIs. It is not supported on UNIs. If necessary, use the **port-type** {**eni** | **nni**} interface configuration command to change the port type.
Step 3	**no shutdown**	If necessary, enable the port. By default NNIs are enabled, and ENIs and UNIs are disabled.
Step 4	**lldp transmit**	LLDP packets are sent on the interface.
Step 5	**lldp receive**	LLDP packets are received on the interface.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

This example shows how to enable LLDP on an interface:

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet1/0/1
Switch(config-if)# no shutdown
Switch(config-if)# port-type nni
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 8-1.

Table 8-1 LLDP-MED TLVs

LLDP-MED TLV	Description
inventory-management	LLDP-MED inventory management TLV

Table 8-1 LLDP-MED TLVs (continued)

LLDP-MED TLV	Description
network-policy	LLDP-MED network policy TLV
power-management	LLDP-MED power management TLV

Disabling a TLV

BEFORE YOU BEGIN

Review the "Information About LLDP and LLDP-MED" section on page 8-1.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface on which you are configuring a LLDP-MED TLV, and enter interface configuration mode.
Step 3	**no lldp med-tlv-select** *tlv*	Specify the TLV to disable.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

This example shows how to disable a TLV:

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet1/0/1
Switch(config-if)# no lldp med-tlv-select inventory-management
Switch(config-if)# end
```

Enabling a TLV

BEFORE YOU BEGIN

Review the "Information About LLDP and LLDP-MED" section on page 8-1.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface on which you are configuring an LLDP-MED TLV, and enter interface configuration mode.
Step 3	**lldp med-tlv-select** *tlv*	Specify the TLV to enable.

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

EXAMPLE

This example shows how to enable a TLV on an interface:

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet1/0/1
Switch(config-if)# lldp med-tlv-select inventory-management
Switch(config-if)# end
```

Verifying Configuration

Command	Description
clear lldp counters	Reset the traffic counters to zero.
clear lldp table	Delete the LLDP table of information about neighbors.
show lldp	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.
show lldp entry *entry-name*	Display information about a specific neighbor. You can enter an asterisk (*) to display all neighbors, or you can enter the name of the neighbor about which you want information.
show lldp interface [*interface-id*]	Display information about interfaces where LLDP is enabled. You can limit the display to the interface about which you want information.
show lldp neighbors [*interface-id*] [**detail**]	Display information about neighbors, including device type, interface type and number, holdtime settings, capabilities, and port ID. You can limit the display to neighbors of a specific interface or expand the display to provide more detailed information.
show lldp traffic	Display LLDP counters, including the number of packets sent and received, number of packets discarded, and number of unrecognized TLVs.

Configuration Example

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
```

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
```

This example shows how to disable LLDP on an interface:

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet1/0/1
Switch(config-if)# no lldp transmit
Switch(config-if)# no lldp receive
Switch(config-if)# end
```

This example shows how to enable LLDP on an interface:

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet1/0/1
Switch(config-if)# no shutdown
Switch(config-if)# port-type nni
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
Switch(config-if)# end
```

This example shows how to disable a TLV:

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet1/0/1
Switch(config-if)# no lldp med-tlv-select inventory-management
Switch(config-if)# end
```

This example shows how to enable a TLV on an interface:

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet1/0/1
Switch(config-if)# lldp med-tlv-select inventory-management
Switch(config-if)# end
```

Related Documents

- Cisco IOS Configuration Fundamentals Command Reference, Release 15.2M&T
- Cisco IOS Master Command List, All Releases

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

Configuring Port-Based Traffic Control

This chapter describes how to configure the port-based traffic control features on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*.

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 9-21.

Information About Port-Based Traffic Control

Port-based traffic control includes the following features:

Storm Control

Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation or in the network configuration can cause a storm.

Storm control (or traffic suppression) monitors packets passing from an interface to the switching bus and determines if the packet is unicast, multicast, or broadcast. The switch counts the number of packets of a specified type received within the 1-second time interval and compares the measurement with a predefined suppression-level threshold.

Storm control uses one of these methods to measure traffic activity:

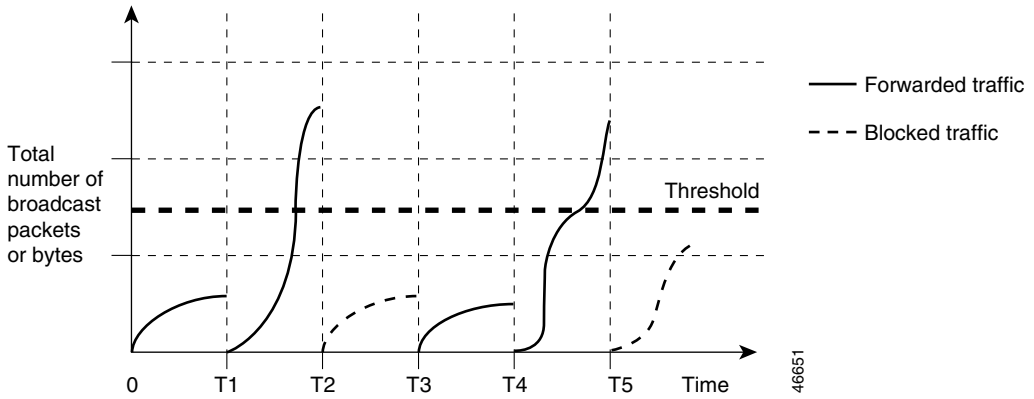
- Bandwidth as a percentage of the total available bandwidth of the port that can be used by the broadcast, multicast, or unicast traffic
- Traffic rate in packets per second at which broadcast, multicast, or unicast packets are received
- Traffic rate in bits per second at which broadcast, multicast, 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.

The graph in Figure 9-1 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 9-1 Broadcast Storm Control Example



The combination of the storm-control suppression level and the 1-second time interval controls 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.

You use the **storm-control** interface configuration commands to set the threshold value for each traffic type.

Protected Ports

Some applications require that no traffic be forwarded at Layer 2 between ports on the same switch so that one neighbor does not see the traffic generated by another neighbor. In such an environment, the use of protected ports ensures that there is no exchange of unicast, broadcast, or multicast traffic between these ports on the switch.

Note NNIs default to non-protected ports. Since UNIs and ENIs s provide port isolation, protected port is not available on UNI and ENI ports. For more information about port types, see the "UNI, NNI, and ENI Port Types" section in *Interfaces Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*.

Protected ports have these features:

- A protected port does not forward any traffic (unicast, multicast, or broadcast) to any other port that is also a protected port. Data traffic cannot be forwarded between protected ports at Layer 2; only control traffic, such as PIM packets, is forwarded because these packets are processed by the CPU and forwarded in software. All data traffic passing between protected ports must be forwarded through a Layer 3 device.
- Forwarding behavior between a protected port and a nonprotected port proceeds as usual.

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.

Port Security

This section includes the following topics:

Secure MAC Addresses

You configure the maximum number of secure addresses allowed on a port by using the **switchport port-security maximum** *value* interface configuration command.

Note If you try to set the maximum value to a number less than the number of secure addresses already configured on an interface, the command is rejected.

The switch supports these types of secure MAC addresses:

- Static secure MAC addresses—These are manually configured by using the **switchport port-security mac-address** *mac-address* interface configuration command, stored in the address table, and added to the switch running configuration.
- Dynamic secure MAC addresses—These are dynamically configured, stored only in the address table, and removed when the switch restarts.
- *Sticky* secure MAC addresses—These can be dynamically learned or manually configured, stored in the address table, and added to the running configuration. If these addresses are saved in the configuration file, when the switch restarts, the interface does not need to dynamically reconfigure them.

You can configure an interface to convert the dynamic MAC addresses to sticky secure MAC addresses and to add them to the running configuration by enabling *sticky learning*. To enable sticky learning, enter the **switchport port-security mac-address sticky** interface configuration command. When you enter this command, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses. All sticky secure MAC addresses are added to the running configuration.

The sticky secure MAC addresses do not automatically become part of the configuration file, which is the startup configuration used each time the switch restarts. If you save the sticky secure MAC addresses in the configuration file, when the switch restarts, the interface does not need to relearn these addresses. If you do not save the sticky secure addresses, they are lost.

If sticky learning is disabled, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration.

The maximum number of secure MAC addresses that you can configure on a switch is set by the maximum number of available MAC addresses allowed in the system. This number is determined by the active Switch Database Management (SDM) template. See Chapter 6, “Configuring SDM Templates.” This number is the total of available MAC addresses, including those used for other Layer 2 functions and any other secure MAC addresses configured on interfaces.

Security Violations

It is a security violation when one of these situations occurs:

- The maximum number of secure MAC addresses have been added to the address table, and a station whose MAC address is not in the address table attempts to access the interface.
- An address learned or configured on one secure interface is seen on another secure interface in the same VLAN.

You can configure the interface for one of three violation modes, based on the action to be taken if a violation occurs:

- protect—when the number of secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred.

  Note We do not recommend configuring the protect violation mode on a trunk port. The protect mode disables learning when any VLAN reaches its maximum limit, even if the port has not reached its maximum limit.

- restrict—when the number of secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. In this mode, you are notified that a security violation has occurred. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.
- shutdown (Default)—a port security violation causes the interface to become error-disabled and to shut down immediately, and the port LED turns off. When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause** *psecure-violation* global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shut down** interface configuration commands.

Table 9-1 shows the violation mode and the actions taken when you configure an interface for port security.

Table 9-1 Security Violation Mode Actions

Violation Mode	Traffic is forwarded[1]	Sends SNMP trap	Sends syslog message	Displays error message[2]	Violation counter increments	Shuts down port
protect	No	No	No	No	No	No
restrict	No	Yes	Yes	No	Yes	No
shutdown	No	No	No	No	Yes	Yes

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.

Prerequisites

Review the "Information About Port-Based Traffic Control" section on page 9-1.

Guidelines and Limitations

Storm Control

- The switch does not require additional configuration to cause the switch storm-control counters to increment for small frames because the storm-control feature correctly handles small frames. 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.

- Storm control is supported on physical interfaces. You can also configure storm control on an EtherChannel. When storm control is configured on an EtherChannel, the storm control settings propagate to the EtherChannel physical interfaces.

Protected Ports

- You can configure protected ports on a physical interface that is configured as an NNI (for example, Gigabit Ethernet port 1) or an EtherChannel group (for example, port-channel 5).
- When you enable protected ports for a port channel, it is enabled for all ports in the port-channel group.
- Do not configure a private-VLAN port as a protected port. Do not configure a protected port as a private-VLAN port. A private-VLAN isolated port does not forward traffic to other isolated ports or community ports.

  For more information about private VLANs, see the “Configuring Private VLANs chapter in the *Layer 2 Switching Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*.

Port Blocking

- 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.
- 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.

Port Security

- Port security can only be configured on static access ports or trunk ports. A secure port cannot be a dynamic access port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- A secure port cannot belong to a Fast EtherChannel or a Gigabit EtherChannel port group.
- A secure port cannot be a private-VLAN port.
- When a trunk port configured with port security and assigned to an access VLAN for data traffic and to a voice VLAN for voice traffic, entering the **switchport voice** and **switchport priority extend** interface configuration commands has no effect.

  When a connected device uses the same MAC address to request an IP address for the access VLAN and then an IP address for the voice VLAN, only the access VLAN is assigned an IP address.
- When you enter a maximum secure address value for an interface, and the new value is greater than the previous value, the new value overwrites the previously configured value. If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.
- The switch does not support port security aging of sticky secure MAC addresses.

Table 9-2 summarizes port security compatibility with other port-based features.

Table 9-2 Port Security Compatibility with Other Switch Features

Type of Port or Feature on Port	Compatible with Port Security
Trunk port	Yes
Dynamic-access port (a VLAN Query Protocol [VQP] port configured with the switchport access vlan dynamic interface configuration command)	No
Routed port	No
SPAN source port	Yes
SPAN destination port	No
EtherChannel	No
Tunneling port	Yes
Protected port	Yes
802.1x port	Yes
Private VLAN port	No
IP source guard	Yes
Dynamic Address Resolution Protocol (ARP) inspection	Yes
Flex Links	Yes

Default Settings

Feature	Default Setting
Storm control	Unicast, broadcast, and multicast storm control are disabled on the switch interfaces; that is, the suppression level is 100 percent.
Protected ports	No protected ports are defined.
Port blocking	Flooding of unknown multicast and unicast traffic out of a port is not blocked; these packets are flooded to all ports.
Port Security Settings	
Port security	Disabled on a port.
Sticky address learning	Disabled.
Maximum number of secure MAC addresses per port	1.
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded.
Port security aging	Disabled. Aging time is 0. Static aging is disabled. Type is absolute.

Configuring Storm Control

You configure storm control on a port and enter the threshold level that you want to be used for a particular type of traffic.

BEFORE YOU BEGIN

Review the "Guidelines and Limitations" section on page 9-5.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface to configure, and enter interface configuration mode.
Step 3	**no shutdown**	Enable the port, if necessary. By default, user network interfaces (UNIs) and enhanced network interfaces (ENIs) are disabled, and network node interfaces (NNIs) are enabled.

	Command	Purpose
Step 4	**storm-control** {**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **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 *level*, specify the rising threshold level for broadcast, multicast, or unicast traffic as a percentage (up to two decimal places) of the bandwidth. The port blocks traffic when the rising threshold is reached. The range is 0.00 to 100.00. • (Optional) For *level-low*, specify the falling threshold level as a percentage (up to two decimal places) of the bandwidth. This value must be less than or equal to the rising suppression value. The port forwards traffic when traffic drops below this level. If you do not configure a falling suppression level, it is set to the rising suppression level. The range is 0.00 to 100.00. If you set the threshold to the maximum value (100 percent), no limit is placed on the traffic. If you set the threshold to 0.0, all broadcast, multicast, and unicast traffic on that port is blocked. • For **bps** *bps*, specify the rising threshold level for broadcast, multicast, or unicast traffic in bits per second (up to one decimal place). The port blocks traffic when the rising threshold is reached. The range is 0.0 to 10000000000.0. • (Optional) For *bps-low*, specify the falling threshold level in bits per second (up to one decimal place). It can be less than or equal to the rising threshold level. The port forwards traffic when traffic drops below this level. The range is 0.0 to 10000000000.0. • For **pps** *pps*, specify the rising threshold level for broadcast, multicast, or unicast traffic in packets per second (up to one decimal place). The port blocks traffic when the rising threshold is reached. The range is 0.0 to 10000000000.0. • (Optional) For *pps-low*, specify the falling threshold level in packets per second (up to one decimal place). It can be less than or equal to the rising threshold level. The port forwards traffic when traffic drops below this level. The range is 0.0 to 10000000000.0. For BPS and PPS settings, you can use metric suffixes such as k, m, and g for large number thresholds.
Step 5	**storm-control action** {**shutdown** | **trap**}	Specify the action to take 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 6	**end**	Return to privileged EXEC mode.

	Command	Purpose
Step 7	**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 8	**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.

EXAMPLE

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 Protected Ports

You can configure protected ports on a physical interface that is configured as an NNI (for example, Gigabit Ethernet port 1) or an EtherChannel group (for example, port-channel 5). When you enable protected ports for a port channel, it is enabled for all ports in the port-channel group.

BEFORE YOU BEGIN

Review the "Guidelines and Limitations" section on page 9-5.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface to configure, and enter interface configuration mode. The interface must be an NNI. **Note** By default, UNIs and ENIs are protected ports.
Step 3	**switchport protected**	Configure the interface to be a protected port.
Step 4	**end**	Return to privileged EXEC mode.

	Command	Purpose
Step 5	**show interfaces** *interface-id* **switchport**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable protected port, use the **no switchport protected** interface configuration command.

EXAMPLE

This example shows how to configure a port as a protected port:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport protected
Switch(config-if)# end
```

This example shows how to configure a FastEthernet port as a protected port:

```
Switch# configure terminal
Switch(config)# interface fastethernet 0/1
Switch(config-if)# port-type NNI
Switch(config-if)# no shutdown
Switch(config-if)# switchport protected
Switch(config-if)# end
```

Configuring Port Blocking

Follow this procedure to disable the flooding of unicast and Layer 2 multicast packets out of an interface.

BEFORE YOU BEGIN

Review the "Guidelines and Limitations" section on page 9-5.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface to configure, and enter interface configuration mode.
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.
Step 4	**switchport block multicast**	Block unknown multicast forwarding out of the port. **Note** Only pure Layer 2 multicast traffic is blocked. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.
Step 5	**switchport block unicast**	Block unknown unicast forwarding out of the port.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show interfaces** *interface-id* **switchport**	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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.

EXAMPLE

This example shows how to block unicast and Layer 2 multicast flooding on a port:

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# no shutdown
Switch(config-if)# switchport block multicast
Switch(config-if)# switchport block unicast
Switch(config-if)# end
```

Configuring Port Security

You can use the port security feature to restrict input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port. When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the workstation attached to that port is assured the full bandwidth of the port.

If a port is configured as a secure port and the maximum number of secure MAC addresses is reached, when the MAC address of a station attempting to access the port is different from any of the identified secure MAC addresses, a security violation occurs. Also, if a station with a secure MAC address configured or learned on one secure port attempts to access another secure port, a violation is flagged.

This section includes the following topics:

Enabling and Configuring Port Security

Follow this procedure to restrict input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port.

BEFORE YOU BEGIN

Review the "Guidelines and Limitations" section on page 9-5.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface to configure, and enter interface configuration mode.
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.

	Command	Purpose
Step 4	**switchport mode** {**access** | **trunk**}	Set the interface switchport mode as access or trunk; an interface in the default mode (dynamic auto) cannot be configured as a secure port.
Step 5	**switchport port-security**	Enable port security on the interface.
Step 6	**switchport port-security** [**maximum** *value* [**vlan** *vlan-list* | **access**]	(Optional) Set the maximum number of secure MAC addresses for the interface. The maximum number of secure MAC addresses that you can configure on a switch is set by the maximum number of available MAC addresses allowed in the system. This number is set by the active Switch Database Management (SDM) template. See Chapter 6, "Configuring SDM Templates." This number is the total of available MAC addresses, including those used for other Layer 2 functions and any other secure MAC addresses configured on interfaces. (Optional) **vlan**—set a per-VLAN maximum value. Enter one of these options after you enter the **vlan** keyword: • *vlan-list*—On a trunk port, you can set a per-VLAN maximum value on a range of VLANs separated by a hyphen or a series of VLANs separated by commas. For nonspecified VLANs, the per-VLAN maximum value is used. • **access**—On an access port, specify the VLAN as an access VLAN.

	Command	Purpose
Step 7	**switchport port-security violation** {**protect** | **restrict** | **shutdown**}	(Optional) Set the violation mode, the action to be taken when a security violation is detected, as one of these: • **protect**—When the number of port secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred. **Note** We do not recommend configuring the protect mode on a trunk port. The protect mode disables learning when any VLAN reaches its maximum limit, even if the port has not reached its maximum limit. • **restrict**—When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. An SNMP trap is sent, a syslog message is logged, and the violation counter increments. • **shutdown**—(Default) The interface is error-disabled when a violation occurs, and the port LED turns off. An SNMP trap is sent, a syslog message is logged, and the violation counter increments. **Note** When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure-violation** global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shutdown** interface configuration commands.
Step 8	**switchport port-security** [**mac-address** *mac-address* [**vlan** {*vlan-id* | {**access**}}]	(Optional) Enter a secure MAC address for the interface. You can use this command to enter the maximum number of secure MAC addresses. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned. **Note** If you enable sticky learning after you enter this command, the secure addresses that were dynamically learned are converted to sticky secure MAC addresses and are added to the running configuration. (Optional) **vlan**—set a per-VLAN maximum value. Enter one of these options after you enter the **vlan** keyword: • *vlan-id*—On a trunk port, you can specify the VLAN ID and the MAC address. If you do not specify a VLAN ID, the native VLAN is used. • **access**—On an access port, specify the VLAN as an access VLAN.
Step 9	**switchport port-security mac-address sticky**	(Optional) Enable sticky learning on the interface.

	Command	Purpose
Step 10	**switchport port-security mac-address sticky** [*mac-address* | **vlan** {*vlan-id* | {**access**}]	(Optional) Enter a sticky secure MAC address, repeating the command as many times as necessary. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned, are converted to sticky secure MAC addresses, and are added to the running configuration. **Note** If you do not enable sticky learning before this command is entered, an error message appears, and you cannot enter a sticky secure MAC address. (Optional) **vlan**—set a per-VLAN maximum value. Enter one of these options after you enter the **vlan** keyword: • *vlan-id*—On a trunk port, you can specify the VLAN ID and the MAC address. If you do not specify a VLAN ID, the native VLAN is used. • **access**—On an access port, specify the VLAN as an access VLAN.
Step 11	**end**	Return to privileged EXEC mode.
Step 12	**show port-security**	Verify your entries.
Step 13	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return the interface to the default condition as not a secure port, use the **no switchport port-security** interface configuration command. If you enter this command when sticky learning is enabled, the sticky secure addresses remain part of the running configuration but are removed from the address table. All addresses are now dynamically learned.

To return the interface to the default number of secure MAC addresses, use the **no switchport port-security maximum** *value* interface configuration command. To return the violation mode to the default condition (shutdown mode), use the **no switchport port-security violation** {**protocol** | **restrict**} interface configuration command.

To disable sticky learning on an interface, use the **no switchport port-security mac-address sticky** interface configuration command. The interface converts the sticky secure MAC addresses to dynamic secure addresses. However, if you have previously saved the configuration with the sticky MAC addresses, you should save the configuration again after entering the **no switchport port-security mac-address sticky** command, or the sticky addresses will be restored if the switch reboots.

Use the **clear port-security {all | configured | dynamic | sticky}** privileged EXEC command to delete from the MAC address table all secure addresses or all secure addresses of a specific type (configured, dynamic, or sticky) on the switch or on an interface.

To delete a specific secure MAC address from the address table, use the **no switchport port-security mac-address** *mac-address* interface configuration command.

To delete all dynamic secure addresses on an interface from the address table, enter the **no switchport port-security** interface configuration command followed by the **switchport port-security** command (to re-enable port security on the interface). If you use the **no switchport port-security mac-address sticky** interface configuration command to convert sticky secure MAC addresses to dynamic secure MAC addresses before entering the **no switchport port-security** command, all secure addresses on the interface except those that were manually configured are deleted.

You must specifically delete configured secure MAC addresses from the address table by using the **no switchport port-security mac-address** *mac-address* interface configuration command.

EXAMPLE

This example shows how to enable port security on a port and to set the maximum number of secure addresses to 50. The violation mode is the default, no static secure MAC addresses are configured, and sticky learning is enabled.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 50
Switch(config-if)# switchport port-security mac-address sticky
```

This example shows how to configure a static secure MAC address on VLAN 3 on a port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 0000.02000.0004 vlan 3
```

This example shows how to enable sticky port security on a port, manually configure MAC addresses for data VLAN, and set the total maximum number of secure addresses to 10:

```
Switch(config)# interface FastEthernet0/1
Switch(config-if)# no shutdown
Switch(config-if)# switchport access vlan 21
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 10
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0002
Switch(config-if)# switchport port-security mac-address 0000.0000.0003
Switch(config-if)# switchport port-security maximum 10 vlan access
```

Enabling and Configuring Port Security Aging

You can use port security aging to set the aging time for all secure addresses on a port. Two types of aging are supported per port:

- Absolute—The secure addresses on the port are deleted after the specified aging time.
- Inactivity—The secure addresses on the port are deleted only if the secure addresses are inactive for the specified aging time.

Use this feature to remove and add devices on a secure port without manually deleting the existing secure MAC addresses and to still limit the number of secure addresses on a port. You can enable or disable the aging of secure addresses on a per-port basis.

BEFORE YOU BEGIN

Review the "Guidelines and Limitations" section on page 9-5.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface to configure, and enter interface configuration mode.
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.
Step 4	**switchport port-security aging** {**static** | **time** *time* | **type** {**absolute** | **inactivity**}}	Enable or disable static aging for the secure port, or set the aging time or type. **Note** The switch does not support port security aging of sticky secure addresses. Enter **static** to enable aging for statically configured secure addresses on this port. For *time*, specify the aging time for this port. The valid range is from 0 to 1440 minutes. For **type**, select one of these keywords: • **absolute**—Sets the aging type as absolute aging. All the secure addresses on this port age out exactly after the time (minutes) specified lapses and are removed from the secure address list. • **inactivity**—Sets the aging type as inactivity aging. The secure addresses on this port age out only if there is no data traffic from the secure source addresses for the specified time period.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show port-security** [**interface** *interface-id*] [**address**]	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable port security aging for all secure addresses on a port, use the **no switchport port-security aging time** interface configuration command. To disable aging for only statically configured secure addresses, use the **no switchport port-security aging static** interface configuration command.

EXAMPLE

This example shows how to set the aging time as 2 hours for the secure addresses on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport port-security aging time 120
```

This example shows how to set the aging time as 2 minutes for the inactivity aging type with aging enabled for the configured secure addresses on the interface:

```
Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```

You can verify the previous commands by entering the **show port-security interface** *interface-id* privileged EXEC command.

Port Security and Private VLANs

Port security allows an administrator to limit the number of MAC addresses learned on a port or to define which MAC addresses can be learned on a port. Follow this procedure to configure port security on a PVLAN host and promiscuous ports.

BEFORE YOU BEGIN

Review the "Guidelines and Limitations" section on page 9-5.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface to configure, and enter interface configuration mode.
Step 3	**switchport mode private-vlan** {**host** | **promiscuous**}	Enable a private VLAN on the interface.
Step 4	**switchport port-security**	Enable port security on the interface.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show port-security** [**interface** *interface-id*] [**address**]	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

```
Switch(config)# interface GigabitEthernet0/8
Switch(config-if)# switchport private-vlan mapping 2061 2201-2206,3101
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport port-security maximum 288
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security violation restrict
```

Note Ports that have both port security and private VLANs configured can be labeled secure PVLAN ports. When a secure address is learned on a secure PVLAN port, the same secure address cannot be learned on another secure PVLAN port belonging to the same primary VLAN. However, an address learned on an unsecure PVLAN port can be learned on a secure PVLAN port belonging to same primary VLAN.

Secure addresses that are learned on host port get automatically replicated on associated primary VLANs, and similarly, secure addresses learned on promiscuous ports automatically get replicated on all associated secondary VLANs. Static addresses (using the **mac-address-table static** command) cannot be user configured on a secure port.

Verifying Configuration

The **show interfaces** *interface-id* **switchport** privileged EXEC command displays (among other characteristics) the interface traffic suppression and control configuration. The **show storm-control** and **show port-security** privileged EXEC commands display those storm control and port security settings.

Command	Purpose
show interfaces [*interface-id*] **switchport**	Displays the administrative and operational status of all switching (nonrouting) ports or the specified port, including port blocking and port protection settings.
show storm-control [*interface-id*] [**broadcast** | **multicast** | **unicast**]	Displays storm control suppression levels set on all interfaces or the specified interface for the specified traffic type or for broadcast traffic if no traffic type is entered.
show port-security [**interface** *interface-id*]	Displays port security settings for the switch or for the specified interface, including the maximum allowed number of secure MAC addresses for each interface, the number of secure MAC addresses on the interface, the number of security violations that have occurred, and the violation mode.
show port-security [**interface** *interface-id*] **address**	Displays all secure MAC addresses configured on all switch interfaces or on a specified interface with aging information for each address.
show port-security interface *interface-id* **vlan**	Displays the number of secure MAC addresses configured per VLAN on the specified interface.

Configuration Example

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
```

This example shows how to configure a port as a protected port:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport protected
Switch(config-if)# end
```

This example shows how to configure a FastEthernet port as a protected port:

```
Switch# configure terminal
Switch(config)# interface fastethernet 0/1
Switch(config-if)# port-type NNI
```

```
Switch(config-if)# no shutdown
Switch(config-if)# switchport protected
Switch(config-if)# end
```

This example shows how to block unicast and Layer 2 multicast flooding on a port:

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# no shutdown
Switch(config-if)# switchport block multicast
Switch(config-if)# switchport block unicast
Switch(config-if)# end
```

This example shows how to enable port security on a port and to set the maximum number of secure addresses to 50. The violation mode is the default, no static secure MAC addresses are configured, and sticky learning is enabled.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 50
Switch(config-if)# switchport port-security mac-address sticky
```

This example shows how to configure a static secure MAC address on VLAN 3 on a port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 0000.02000.0004 vlan 3
```

This example shows how to enable sticky port security on a port, manually configure MAC addresses for data VLAN, and set the total maximum number of secure addresses to 10:

```
Switch(config)# interface FastEthernet0/1
Switch(config-if)# no shutdown
Switch(config-if)# switchport access vlan 21
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 10
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0002
Switch(config-if)# switchport port-security mac-address 0000.0000.0003
Switch(config-if)# switchport port-security maximum 10 vlan access
```

This example shows how to set the aging time as 2 hours for the secure addresses on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport port-security aging time 120
```

This example shows how to set the aging time as 2 minutes for the inactivity aging type with aging enabled for the configured secure addresses on the interface:

```
Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```

This example shows how to configure port security on a PVLAN:

```
Switch(config)# interface GigabitEthernet0/8
Switch(config-if)# switchport private-vlan mapping 2061 2201-2206,3101
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport port-security maximum 288
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security violation restrict
```

Related Documents

- Cisco IOS Master Command List, All Releases
- Cisco IOS Interface and Hardware Component Command Reference
- Interfaces Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches
- Layer 2 Switching Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

Configuring CDP

This chapter describes how to configure Cisco Discovery Protocol (CDP) on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*.

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 10-7.

Information About 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 hold time 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.

Prerequisites

Interfaces must support Subnetwork Access Protocol (SNAP) headers.

Guidelines and Limitations

- Cisco Discovery Protocol functions only on Cisco devices.
- Cisco Discovery Protocol is not supported on Frame Relay multipoint subinterfaces.

Default Settings

Feature	Default Setting
CDP global state	Enabled.
CDP interface state	Enabled only on NNIs; disabled on ENIs. **Note** CDP is not supported on UNIs.
CDP timer (packet update frequency)	60 seconds.
CDP holdtime (before discarding)	180 seconds.
CDP Version-2 advertisements	Enabled.

Configuring CDP

This section includes the following topics:

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.

CDP packets are sent with a time to live, or hold time, value. The receiving device will discard the CDP information in the CDP packet after the hold time has elapsed.

You can set the hold time lower than the default setting of 180 seconds if you want the receiving devices to update their CDP information more rapidly. The CDP hold time must be set to a higher number of seconds than the time between CDP transmissions, which is set using the **cdp timer** command.

BEFORE YOU BEGIN

Steps 2 through 4 are all optional and can be performed in any order.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**cdp timer** *seconds*	(Optional) Set the transmission frequency of CDP updates in seconds. The range is 5 to 254; the default is 60 seconds.
Step 3	**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.
Step 4	**cdp advertise-v2**	(Optional) Configure CDP to send Version-2 advertisements. This is the default state.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show cdp**	Verify your settings.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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

EXAMPLE

This example shows how to configure CDP characteristics:

```
Switch# configure terminal
Switch(config)# cdp timer 50
Switch(config)# cdp holdtime 120
Switch(config)# cdp advertise-v2
Switch(config)# end
```

Disabling and Enabling CDP

CDP is enabled by default on NNIs. It is disabled by default on ENIs but can be enabled.

Disabling CDP

BEFORE YOU BEGIN

Cisco devices (such as Cisco IP phones) regularly exchange CDP messages with connected devices. Disabling CDP can interrupt device connectivity.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no cdp run**	Disable CDP.
Step 3	**end**	Return to privileged EXEC mode.

EXAMPLE

```
Switch# configure terminal
Switch(config)# no cdp run
Switch(config)# end
```

Enabling CDP

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**cdp run**	Enable CDP after disabling it.
Step 3	**end**	Return to privileged EXEC mode.

EXAMPLE

```
Switch# configure terminal
Switch(config)# cdp run
Switch(config)# end
```

Disabling and Enabling CDP on an Interface

CDP is enabled by default on NNIs to send and to receive CDP information. You can enable CDP on ENIs, but it is not supported on UNIs.

Disabling CDP on an Interface

BEFORE YOU BEGIN

Cisco devices (such as Cisco IP phones) regularly exchange CDP messages with connected devices. Disabling CDP can interrupt device connectivity.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface on which you are disabling CDP, and enter interface configuration mode. **Note** If the interface is a UNI, you must enter the **port-type nni** or **port-type eni** interface configuration command before configuring CDP. By default, CDP is enabled on NNIs and disabled on ENIs.
Step 3	**no cdp enable**	Disable CDP on the interface.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no cdp enable
Switch(config-if)# end
```

Enabling CDP on an Interface

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface on which you are enabling CDP, and enter interface configuration mode. **Note** If the interface is a UNI, you must enter the **port-type nni** or **port-type eni** interface configuration command before configuring CDP. By default, CDP is enabled on NNIs and disabled on ENIs.
Step 3	**cdp enable**	Enable CDP on the interface after disabling it.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

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
```

This example shows how to change a UNI to an ENI and enable CDP on the port:

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# port-type eni
Switch(config-if)# cdp enable
Switch(config-if)# end
```

Verifying Configuration

Command	Description
clear cdp counters	Reset the traffic counters to zero.
clear cdp table	Delete the CDP table of information about neighbors.
show cdp	Display global information, such as frequency of transmissions and the hold time for packets being sent.
show cdp entry *entry-name* [**protocol** | **version**]	Display information about a specific neighbor. You can enter an asterisk (*) to display all CDP neighbors, or you can enter the name of the neighbor about which you want information. You can also limit the display to information about the protocols enabled on the specified neighbor or information about the version of software running on the device.
show cdp interface [*interface-id*]	Display information about interfaces where CDP is enabled. You can limit the display to the interface about which you want information.
show cdp neighbors [*interface-id*] [**detail**]	Display information about neighbors, including device type, interface type and number, hold time 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.
show cdp traffic	Display CDP counters, including the number of packets sent and received and checksum errors.

Configuration Example

This example shows how to configure CDP characteristics:

```
Switch# configure terminal
Switch(config)# cdp timer 50
Switch(config)# cdp holdtime 120
Switch(config)# cdp advertise-v2
Switch(config)# end
```

This example shows how to globally enable CDP if it has been disabled:

```
Switch# configure terminal
```

```
Switch(config)# cdp run
Switch(config)# end
```

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
```

This example shows how to change a UNI to an ENI and enable CDP on the port:

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# port-type eni
Switch(config-if)# cdp enable
Switch(config-if)# end
```

Related Documents

- Cisco IOS Master Command List, All Releases
- Cisco IOS Cisco Discovery Protocol Command Reference
- Cisco Discovery Protocol Configuration Guide, Cisco IOS Release 15M&T

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

Configuring SPAN and RSPAN

This chapter describes how to configure Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*.

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 11-26.

Information About SPAN and RSPAN

You can analyze network traffic passing through ports or VLANs by using SPAN or RSPAN to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer or other monitoring or security device. SPAN copies (or mirrors) traffic received or sent (or both) on source ports or source VLANs to a destination port for analysis. SPAN does not affect the switching of network traffic on the source ports or VLANs. You must dedicate the destination port for SPAN use. Except for traffic that is required for the SPAN or RSPAN session, destination ports do not receive or forward traffic.

Only traffic that enters or leaves source ports or traffic that enters or leaves source VLANs can be monitored by using SPAN; traffic routed to a source VLAN cannot be monitored. For example, if incoming traffic is being monitored, traffic that gets routed from another VLAN to the source VLAN cannot be monitored; however, traffic that is received on the source VLAN and routed to another VLAN can be monitored.

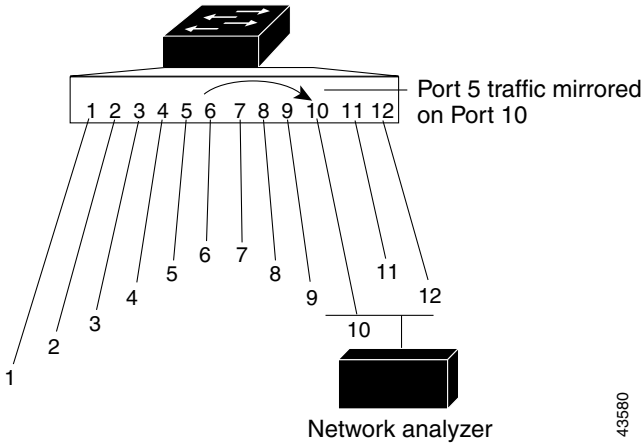
You can use the SPAN or RSPAN destination port to inject traffic from a network security device. For example, if you connect a Cisco Intrusion Detection System (IDS) sensor appliance to a destination port, the IDS device can send TCP reset packets to close down the TCP session of a suspected attacker.

This section includes the following topics:

Local SPAN

Local SPAN supports a SPAN session entirely within one switch; all source ports or source VLANs and destination ports reside in the same switch. Local SPAN copies traffic from one or more source ports in any VLAN or from one or more VLANs to a destination port for analysis. For example, in Figure 11-1, all traffic on port 5 (the source port) is mirrored to port 10 (the destination port). A network analyzer on port 10 receives all network traffic from port 5 without being physically attached to port 5.

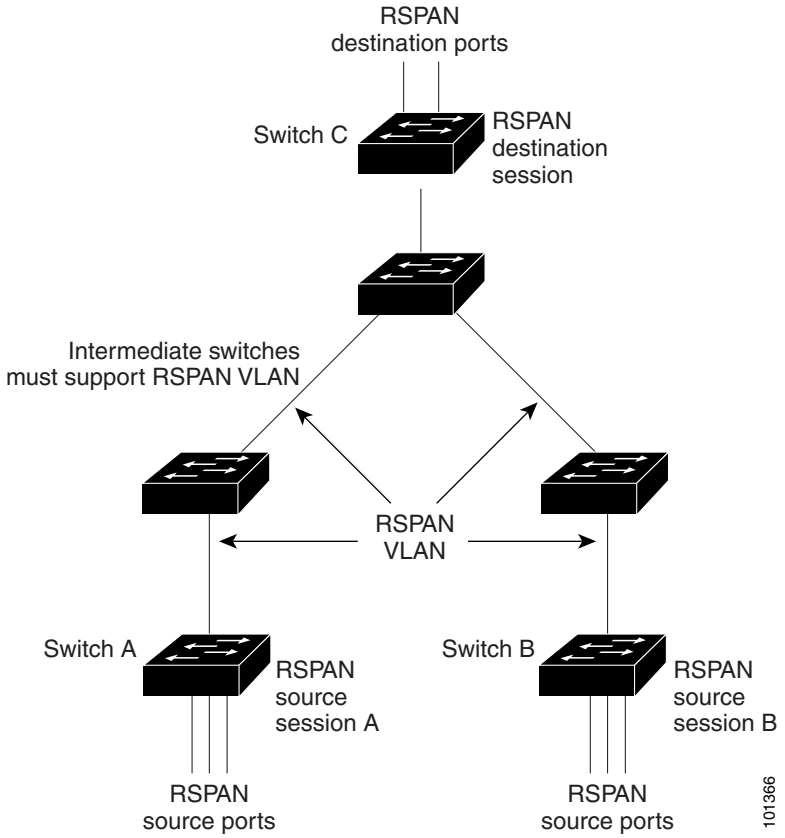
Figure 11-1 Example of Local SPAN Configuration on a Single Switch



Remote SPAN

RSPAN supports source ports, source VLANs, and destination ports on different switches, enabling remote monitoring of multiple switches across your network. Figure 11-2 shows source ports on Switch A and Switch B. The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches. The RSPAN traffic from the source ports or VLANs is copied into the RSPAN VLAN and forwarded over trunk ports carrying the RSPAN VLAN to a destination session monitoring the RSPAN VLAN. Each RSPAN source switch must have either ports or VLANs as RSPAN sources. The destination is always a physical port, as shown on Switch C in the figure.

Figure 11-2 Example of RSPAN Configuration



SPAN and RSPAN Concepts and Terminology

This section describes concepts and terminology associated with SPAN and RSPAN configuration.

SPAN Sessions

SPAN sessions (local or remote) allow you to monitor traffic on one or more ports, or one or more VLANs, and send the monitored traffic to one or more destination ports.

A local SPAN session is an association of a destination port with source ports or source VLANs, all on a single network device. Local SPAN does not have separate source and destination sessions. Local SPAN sessions gather a set of ingress and egress packets specified by the user and form them into a stream of SPAN data, which is directed to the destination port.

RSPAN consists of at least one RSPAN source session, an RSPAN VLAN, and at least one RSPAN destination session. You separately configure RSPAN source sessions and RSPAN destination sessions on different network devices. To configure an RSPAN source session on a device, you associate a set of source ports or source VLANs with an RSPAN VLAN. The output of this session is the stream of SPAN packets that are sent to the RSPAN VLAN. To configure an RSPAN destination session on another device, you associate the destination port with the RSPAN VLAN. The destination session collects all RSPAN VLAN traffic and sends it out the RSPAN destination port.

An RSPAN source session is very similar to a local SPAN session, except for where the packet stream is directed. In an RSPAN source session, SPAN packets are relabeled with the RSPAN VLAN ID and directed over normal trunk ports to the destination switch.

An RSPAN destination session takes all packets received on the RSPAN VLAN, strips off the VLAN tagging, and presents them on the destination port. Its purpose is to present a copy of all RSPAN VLAN packets (except Layer 2 control packets) to the user for analysis.

There can be more than one source session and more than one destination session active in the same RSPAN VLAN. There can also be intermediate switches separating the RSPAN source and destination sessions. These switches need not be capable of running RSPAN, but they must respond to the requirements of the RSPAN VLAN (see the "RSPAN VLAN" section on page 11-7).

Traffic monitoring in a SPAN session has these restrictions:

- Sources can be ports or VLANs, but you cannot mix source ports and source VLANs in the same session.
- The switch supports up to two source sessions (local SPAN and RSPAN source sessions). You can run both a local SPAN and an RSPAN source session in the same switch. The switch supports a total of 66 source and RSPAN destination sessions.
- You can have multiple destination ports in a SPAN session, but no more than 64 destination ports.
- You can configure two separate SPAN or RSPAN source sessions with separate or overlapping sets of SPAN source ports and VLANs. When the LAN Base image is running on the switch, both switched and routed ports can be configured as SPAN sources and destinations.
- SPAN sessions do not interfere with the normal operation of the switch. However, an oversubscribed SPAN destination, for example, a 10-Mbps port monitoring a 100-Mbps port, can result in dropped or lost packets.
- When RSPAN is enabled, each packet being monitored is transmitted twice, once as normal traffic and once as a monitored packet. Therefore monitoring a large number of ports or VLANs could potentially generate large amounts of network traffic.
- You can configure SPAN sessions on disabled ports; however, a SPAN session does not become active unless you enable the destination port and at least one source port or VLAN for that session.
- The switch does not support a combination of local SPAN and RSPAN in a single session. That is, an RSPAN source session cannot have a local destination port, an RSPAN destination session cannot have a local source port, and an RSPAN destination session and an RSPAN source session that are using the same RSPAN VLAN cannot run on the same switch.

Monitored Traffic

SPAN sessions can monitor these traffic types:

- Receive (Rx) SPAN—The goal of receive (or ingress) SPAN is to monitor as much as possible all the packets received by the source interface or VLAN before any modification or processing is performed by the switch. A copy of each packet received by the source is sent to the destination port for that SPAN session.

  Packets that are modified because of routing or quality of service (QoS)—for example, modified Differentiated Services Code Point (DSCP)—are copied before modification.

  Features that can cause a packet to be dropped during receive processing have no effect on ingress SPAN; the destination port receives a copy of the packet even if the actual incoming packet is dropped. These features include IP standard and extended input access control lists (ACLs), ingress QoS policing, VLAN ACLs and egress QoS policing.

- Transmit (Tx) SPAN—The goal of transmit (or egress) SPAN is to monitor as much as possible all the packets sent by the source interface after all modification and processing is performed by the switch. A copy of each packet sent by the source is sent to the destination port for that SPAN session. The copy is provided after the packet is modified.

  Packets that are modified because of routing—for example, with modified time-to-live (TTL), MAC-address, or QoS values—are duplicated (with the modifications) at the destination port.

  Features that can cause a packet to be dropped during transmit processing also affect the duplicated copy for SPAN. These features include IP standard and extended output ACLs and egress QoS policing.

- Both—In a SPAN session, you can also monitor a port or VLAN for both received and sent packets. This is the default.

The default configuration for local SPAN session ports is to send all packets untagged. SPAN also does not normally monitor bridge protocol data unit (BPDU) packets and Layer 2 protocols, such as Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), and Port Aggregation Protocol (PAgP). However, when you enter the **encapsulation replicate** keywords when configuring a destination port, these changes occur:

- Packets are sent on the destination port with the same encapsulation—untagged or IEEE 802.1Q—that they had on the source port.
- Packets of all types, including BPDU and Layer 2 protocol packets, are monitored.

Therefore, a local SPAN session with encapsulation replicate enabled can have a mixture of untagged and 802.1Q tagged packets appear on the destination port.

Switch congestion can cause packets to be dropped at ingress source ports, egress source ports, or SPAN destination ports. In general, these characteristics are independent of one another. For example:

- A packet might be forwarded normally but dropped from monitoring due to an oversubscribed SPAN destination port.
- An ingress packet might be dropped from normal forwarding, but still appear on the SPAN destination port.
- An egress packet dropped because of switch congestion is also dropped from egress SPAN.

In some SPAN configurations, multiple copies of the same source packet are sent to the SPAN destination port. For example, a bidirectional (both Rx and Tx) SPAN session is configured for the Rx monitor on port A and Tx monitor on port B. If a packet enters the switch through port A and is switched to port B, both incoming and outgoing packets are sent to the destination port. Both packets are the same (unless a Layer-3 rewrite occurs, in which case the packets are different because of the packet modification).

Source Ports

A source port (also called a *monitored port*) is a switched or routed port that you monitor for network traffic analysis. In a local SPAN session or RSPAN source session, you can monitor source ports or VLANs for traffic in one or both directions. The switch supports any number of source ports (up to the maximum number of available ports on the switch) and any number of source VLANs (up to the maximum number of VLANs supported). However, the switch supports a maximum of two sessions (local or RSPAN) with source ports or VLANs, and you cannot mix ports and VLANs in a single session.

A source port has these characteristics:

- It can be monitored in multiple SPAN sessions.
- Each source port can be configured with a direction (ingress, egress, or both) to monitor.

- It can be any port type—for example, EtherChannel, Fast Ethernet, Gigabit Ethernet, user network interface (UNI), network node interface (NNI), enhanced network interface (ENI) and so forth.
- For EtherChannel sources, you can monitor traffic for the entire EtherChannel or individually on a physical port as it participates in the port channel.
- It can be a routed port, an access port, or a trunk port.
- It cannot be a destination port.
- Source ports can be in the same or different VLANs.
- You can monitor multiple source ports in a single session.

Source VLANs

VLAN-based SPAN (VSPAN) is the monitoring of the network traffic in one or more VLANs. The SPAN or RSPAN source interface in VSPAN is a VLAN ID, and traffic is monitored on all the ports for that VLAN.

VSPAN has these characteristics:

- All active ports in the source VLAN are included as source ports and can be monitored in either or both directions.
- On a given port, only traffic on the monitored VLAN is sent to the destination port.
- If a destination port belongs to a source VLAN, it is excluded from the source list and is not monitored.
- If ports are added to or removed from the source VLANs, the traffic on the source VLAN received by those ports is added to or removed from the sources being monitored.
- You cannot use filter VLANs in the same session with VLAN sources.
- You can monitor only Ethernet VLANs.

VLAN Filtering

When you monitor a trunk port as a source port, by default, all VLANs active on the trunk are monitored. You can limit SPAN traffic monitoring on trunk source ports to specific VLANs by using VLAN filtering.

- VLAN filtering applies only to trunk ports.
- VLAN filtering applies only to port-based sessions and is not allowed in sessions with VLAN sources.
- When a VLAN filter list is specified, only those VLANs in the list are monitored on trunk ports.
- SPAN traffic coming from other port types is not affected by VLAN filtering; that is, all VLANs are allowed on other ports.
- VLAN filtering affects only traffic forwarded to the destination SPAN port and does not affect the switching of normal traffic.

Destination Port

Each local SPAN session or RSPAN destination session must have a destination port (also called a *monitoring port*) that receives a copy of traffic from the source ports or VLANs and sends the SPAN packets to the user, usually a network analyzer.

A destination port has these characteristics:

- For a local SPAN session, the destination port must reside on the same switch as the source port. For an RSPAN session, it is located on the switch containing the RSPAN destination session. There is no destination port on a switch running only an RSPAN source session.
- When a port is configured as a SPAN destination port, the configuration overwrites the original port configuration. When the SPAN destination configuration is removed, the port reverts to its previous configuration. If a configuration change is made to the port while it is acting as a SPAN destination port, the change does not take effect until the SPAN destination configuration had been removed.
- If the port was in an EtherChannel group, it is removed from the group while it is a destination port. If the switch is running the IP services image and the port was a routed port, it is no longer a routed port.
- It can be any Ethernet physical port.
- It cannot be a secure port.
- It cannot be a source port.
- It cannot be an EtherChannel group or a VLAN.
- It can participate in only one SPAN session at a time (a destination port in one SPAN session cannot be a destination port for a second SPAN session).
- When it is active, incoming traffic is disabled. The port does not send any traffic except that required for the SPAN session. Incoming traffic is never learned or forwarded on a destination port.
- If incoming traffic forwarding is enabled for a network security device, the destination port forwards traffic at Layer 2.
- It does not participate in any of the Layer 2 protocols (STP, VTP, CDP, DTP, PagP).
- A destination port that belongs to a source VLAN of any SPAN session is excluded from the source list and is not monitored.
- The maximum number of destination ports in a switch is 64.

Local SPAN and RSPAN destination ports behave differently regarding VLAN tagging and encapsulation:

- For local SPAN, if the **encapsulation replicate** keywords are specified for the destination port, these packets appear with the original encapsulation (untagged or 802.1Q). If **encapsulation dot1q** is specified, packets appear with the 802.1Q encapsulation. If these keywords are not specified, packets appear in the untagged format. Therefore, the output of a local SPAN session with **encapsulation replicate** enabled can contain a mixture of untagged and 802.1Q tagged packets.
- For RSPAN, the original VLAN ID is lost because it is overwritten by the RSPAN VLAN identification. Therefore, all packets appear on the destination port as untagged.

RSPAN VLAN

The RSPAN VLAN carries SPAN traffic between RSPAN source and destination sessions. It has these special characteristics:

- All traffic in the RSPAN VLAN is always flooded.
- No MAC address learning occurs on the RSPAN VLAN.
- RSPAN VLAN traffic only flows on trunk ports.
- RSPAN VLANs must be configured in VLAN configuration mode by using the **remote-span** VLAN configuration mode command.

  - To change a VLAN from a UNI-ENI isolated VLAN (the default) to an RSPAN VLAN, enter the **rspan-vlan** VLAN configuration command.
  - To change a UNI-ENI community VLAN to an RSPAN VLAN, you must first remove the community VLAN type by entering the **no uni-vlan** VLAN configuration command.
- STP can run on RSPAN VLAN trunks but not on SPAN destination ports.

Note NNIs support STP by default and you can enable STP on ENIs. UNIs do not support STP.

- An RSPAN VLAN cannot be a private-VLAN primary or secondary VLAN.

It is normal to have multiple RSPAN VLANs in a network at the same time with each RSPAN VLAN defining a network-wide RSPAN session. That is, multiple RSPAN source sessions anywhere in the network can contribute packets to the RSPAN session. It is also possible to have multiple RSPAN destination sessions throughout the network, monitoring the same RSPAN VLAN and presenting traffic to the user. The RSPAN VLAN ID separates the sessions.

Prerequisites

Review the "Information About SPAN and RSPAN" section on page 11-1 and "SPAN and RSPAN Interaction with Other Features" section on page 11-9.

Guidelines and Limitations

SPAN Configuration Guidelines

- You can configure a total of two local SPAN sessions or RSPAN source sessions on each switch. You can have a total of 66 SPAN sessions (local, RSPAN source, and RSPAN destination) on a switch.
- For SPAN sources, you can monitor traffic for a single port or VLAN or a series or range of ports or VLANs for each session. You cannot mix source ports and source VLANs within a single SPAN session.
- The destination port cannot be a source port; a source port cannot be a destination port.
- You cannot have two SPAN sessions using the same destination port.
- When you configure a switch port as a SPAN destination port, it is no longer a normal switch port; only monitored traffic passes through the SPAN destination port.
- Entering SPAN configuration commands does not remove previously configured SPAN parameters. You must enter the **no monitor session** {*session_number* | **all** | **local** | **remote**} global configuration command to delete configured SPAN parameters.
- For local SPAN, outgoing packets through the SPAN destination port carry the original encapsulation headers—untagged or 802.1Q—if the **encapsulation replicate** or **encapsulation dot1q** keywords are specified. If the keywords are not specified, the packets are sent in native form. For RSPAN destination ports, outgoing packets are not tagged.
- You can configure a disabled port to be a source or destination port, but the SPAN function does not start until the destination port and at least one source port or source VLAN are enabled.

- You can limit SPAN traffic to specific VLANs by using the **filter vlan** keyword. If a trunk port is being monitored, only traffic on the VLANs specified with this keyword is monitored. By default, all VLANs are monitored on a trunk port.
- You cannot mix source VLANs and filter VLANs within a single SPAN session.

RSPAN Configuration Guidelines

- All SPAN configuration guidelines apply to RSPAN.
- As RSPAN VLANs have special properties, you should reserve a few VLANs across your network for use as RSPAN VLANs; do not assign access ports to these VLANs.
- You can apply an output ACL to RSPAN traffic to selectively filter or monitor specific packets. Specify these ACLs on the RSPAN VLAN in the RSPAN source switches.
- For RSPAN configuration, you can distribute the source ports and the destination ports across multiple switches in your network.
- RSPAN does not support BPDU packet monitoring or other Layer 2 switch protocols.
- The RSPAN VLAN is configured only on trunk ports and not on access ports. To avoid unwanted traffic in RSPAN VLANs, make sure that the VLAN remote-span feature is supported in all the participating switches.
- Access ports on the RSPAN VLAN are put in the inactive state.
- RSPAN VLANs are included as sources for port-based RSPAN sessions when source trunk ports have active RSPAN VLANs. RSPAN VLANs can also be sources in SPAN sessions. However, since the switch does not monitor spanned traffic, it does not support egress spanning of packets on any RSPAN VLAN identified as the destination of an RSPAN source session on the switch.
- You can configure any VLAN as an RSPAN VLAN as long as these conditions are met:
  - The same RSPAN VLAN is used for an RSPAN session in all the switches.
  - All participating switches support RSPAN.
  - MAC address learning is not disabled on the RSPAN VLAN.
- We recommend that you configure an RSPAN VLAN before you configure an RSPAN source or a destination session.

SPAN and RSPAN Interaction with Other Features

- Routing—For switches that are running the IP services image, SPAN does not monitor routed traffic. RSPAN only monitors traffic that enters or exits the switch, not traffic that is routed between VLANs. For example, if a VLAN is being receive-monitored and the switch routes traffic from another VLAN to the monitored VLAN, that traffic is not monitored and is not received on the SPAN destination port.
- STP—A destination port does not participate in STP while its SPAN or RSPAN session is active. The destination port can participate in STP after the SPAN or RSPAN session is disabled. On a source port, SPAN does not affect the STP status. STP can be active on trunk ports carrying an RSPAN VLAN. However, only NNIs or ENIs can support STP; UNIs do not participate in STP.
- CDP—A SPAN destination port does not participate in CDP while the SPAN session is active. After the SPAN session is disabled, the port again participates in CDP. NNIs have CDP enabled by default and you can enable it on ENIs; UNIs do not participate in CDP.

- VLAN and trunking—You can modify VLAN membership or trunk settings for source or destination ports at any time. However, changes in VLAN membership or trunk settings for a destination port do not take effect until you remove the SPAN destination configuration. Changes in VLAN membership or trunk settings for a source port immediately take effect, and the respective SPAN sessions automatically adjust accordingly.
- EtherChannel—You can configure an EtherChannel group as a source port but not as a SPAN destination port. When a group is configured as a SPAN source, the entire group is monitored.

  If a physical port is added to a monitored EtherChannel group, the new port is added to the SPAN source port list. If a port is removed from a monitored EtherChannel group, it is automatically removed from the source port list.

  A physical port that belongs to an EtherChannel group can be configured as a SPAN source port and still be a part of the EtherChannel. In this case, data from the physical port is monitored as it participates in the EtherChannel. However, if a physical port that belongs to an EtherChannel group is configured as a SPAN destination, it is removed from the group. After the port is removed from the SPAN session, it rejoins the EtherChannel group. Ports removed from an EtherChannel group remain members of the group, but they are in the *inactive* or *suspended* state.

  If a physical port that belongs to an EtherChannel group is a destination port and the EtherChannel group is a source, the port is removed from the EtherChannel group and from the list of monitored ports.
- Multicast traffic can be monitored. For sending and receiving port monitoring, only a single unedited packet is sent to the SPAN destination port. It does not reflect the number of times that the multicast packet is sent.
- A private-VLAN port cannot be a SPAN destination port.
- A secure port cannot be a SPAN destination port.

  For SPAN sessions, do not enable port security on ports with monitored egress when ingress forwarding is enabled on the destination port. For RSPAN source sessions, do not enable port security on any ports with monitored egress.
- An 802.1x port can be a SPAN source port. You can enable 802.1x on a port that is a SPAN destination port; however, 802.1x is disabled until the port is removed as a SPAN destination.

  For SPAN sessions, do not enable 802.1x on ports with monitored sending when receive forwarding is enabled on the destination port. For RSPAN source sessions, do not enable IEEE 802.1x on any ports that are sending monitored.

Default Settings

Feature	Default Setting
SPAN state (SPAN and RSPAN)	Disabled.
Source port traffic to monitor	Both received and sent traffic (**both**).
Encapsulation type (destination port)	Native form (untagged packets).
Ingress forwarding (destination port)	Disabled.

Feature	Default Setting
VLAN filtering	On a trunk interface used as a source port, all VLANs are monitored.
RSPAN VLANs	None configured. Default VLAN type is UNI-ENI isolated.

Configuring SPAN and RSPAN

Configuring Local SPAN

Creating a Local SPAN Session

Follow this procedure to create a SPAN session and specify the source (monitored) ports or VLANs and the destination (monitoring) ports:

BEFORE YOU BEGIN

Review the "Information About SPAN and RSPAN" section on page 11-1 and "Guidelines and Limitations" section on page 11-8.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	Remove any existing SPAN configuration for the session. For *session_number*, the range is 1 to 66. Specify **all** to remove all SPAN sessions, **local** to remove all local sessions, or **remote** to remove all remote SPAN sessions.

	Command	Purpose
Step 3	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]	Specify the SPAN session and the source port (monitored port). For *session_number*, the range is 1 to 66. For *interface-id*, specify the source port or source VLAN to monitor. • For source *interface-id*, specify the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (**port-channel** *port-channel-number*). Valid port-channel numbers are 1 to 48. • For *vlan-id*, specify the source VLAN to monitor. The range is 1 to 4094 (excluding the RSPAN VLAN). **Note** A single session can include multiple sources (ports or VLANs), defined in a series of commands, but you cannot combine source ports and source VLANs in one session. (Optional) [**,** | **-**] Specify a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen. (Optional) Specify the direction of traffic to monitor. If you do not specify a traffic direction, the SPAN monitors both sent and received traffic. • **both**—Monitor both received and sent traffic. This is the default. • **rx**—Monitor received traffic. • **tx**—Monitor sent traffic. **Note** You can use the **monitor session** *session_number* **source** command multiple times to configure multiple source ports.

	Command	Purpose
Step 4	**monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation**{**dot1q** | **replicate**}]	Specify the SPAN session and the destination port (monitoring port). For *session_number*, specify the session number entered in Step 3. **Note** For local SPAN, you must use the same session number for the source and destination interfaces. For *interface-id*, specify the destination port. The destination interface must be a physical port; it cannot be an EtherChannel, and it cannot be a VLAN. (Optional) [**,** | **-**] Specify a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen. (Optional) Enter **encapsulation dot1q** for 802.1Q encapsulation or **encapsulation replicate** to specify that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged). **Note** You can use **monitor session** *session_number* **destination** command multiple times to configure multiple destination ports.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show monitor** [**session** *session_number*] **show running-config**	Verify the configuration.
Step 7	**copy running-config startup-config**	(Optional) Save the configuration in the configuration file.

To delete a SPAN session, use the **no monitor session** *session_number* global configuration command. To remove a source or destination port or VLAN from the SPAN session, use the **no monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} global configuration command or the **no monitor session** *session_number* **destination interface** *interface-id* global configuration command. For destination interfaces, the **encapsulation replicate** keywords are ignored with the **no** form of the command.

EXAMPLE

This example shows how to set up SPAN session 1 for monitoring source port traffic to a destination port. First, any existing SPAN configuration for session 1 is deleted, and then bidirectional traffic is mirrored from source Gigabit Ethernet port 1 to destination Gigabit Ethernet port 2, retaining the encapsulation method.

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet0/1
Switch(config)# monitor session 1 destination interface gigabitethernet0/2
encapsulation replicate
Switch(config)# end
```

This example shows how to remove port 1 as a SPAN source for SPAN session 1:

```
Switch(config)# no monitor session 1 source interface gigabitethernet0/1
```

```
Switch(config)# end
```

This example shows how to disable received traffic monitoring on port 1, which was configured for bidirectional monitoring:

```
Switch(config)# no monitor session 1 source interface gigabitethernet0/1 rx
```

The monitoring of traffic received on port 1 is disabled, but traffic sent from this port continues to be monitored.

This example shows how to remove any existing configuration on SPAN session 2, configure SPAN session 2 to monitor received traffic on all ports belonging to VLANs 1 through 3, and send it to destination Gigabit Ethernet port 2. The configuration is then modified to also monitor all traffic on all ports belonging to VLAN 10.

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source vlan 1 - 3 rx
Switch(config)# monitor session 2 destination interface gigabitethernet0/2
Switch(config)# monitor session 2 source vlan 10
Switch(config)# end
```

Creating a Local SPAN Session and Configuring Ingress Traffic

Follow this procedure to create a SPAN session, to specify the source ports or VLANs and the destination ports, and to enable ingress traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance).

Note See the "Creating a Local SPAN Session" section on page 11-11 for details about the keywords not related to ingress traffic.

BEFORE YOU BEGIN

Review the "Information About SPAN and RSPAN" section on page 11-1 and "Guidelines and Limitations" section on page 11-8.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	Remove any existing SPAN configuration for the session.
Step 3	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]	Specify the SPAN session and the source port (monitored port).

	Command	Purpose
Step 4	**monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation** {**dot1q** | **replicate**}] [**ingress** {[**dot1q** | **untagged**] **vlan** *vlan-id*}]	Specify the SPAN session, the destination port, the packet encapsulation, and the ingress VLAN and encapsulation. For *session_number*, specify the session number entered in Step 3. For *interface-id*, specify the destination port. The destination interface must be a physical port; it cannot be an EtherChannel, and it cannot be a VLAN. (Optional) **[, | -]** Specify a series or range of interfaces. Enter a space before and after the comma or hyphen. (Optional) Enter **encapsulation dot1q** for 802.1Q encapsulation or **encapsulation replicate** to specify that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged). Enter **ingress** with keywords to enable ingress traffic forwarding on the destination port and specify the encapsulation type: • **dot1q**—Forward incoming packets with 802.1Q encapsulation with the specified VLAN as the default VLAN. • **untagged**—Forward incoming packets with untagged encapsulation type with the specified VLAN as the default VLAN. • **vlan** *vlan-id*—The default VLAN. If neither **dot1q** or **untagged** is specified, the default is to forward packets untagged.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show monitor** [**session** *session_number*] **show running-config**	Verify the configuration.
Step 7	**copy running-config startup-config**	(Optional) Save the configuration in the configuration file.

To delete a SPAN session, use the **no monitor session** *session_number* global configuration command. To remove a source or destination port or VLAN from the SPAN session, use the **no monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} global configuration command or the **no monitor session** *session_number* **destination interface** *interface-id* global configuration command. For destination interfaces, the encapsulation and ingress options are ignored with the **no** form of the command.

EXAMPLE

This example shows how to remove any existing configuration on SPAN session 2, configure SPAN session 2 to monitor sent traffic on Gigabit Ethernet source port 1 and send it to destination Gigabit Ethernet port 2 with the same egress encapsulation type as the source port, and enable incoming forwarding with 802.1Q encapsulation and VLAN 6 as the default ingress VLAN:

```
Switch(config)# no monitor session 2
```

```
Switch(config)# monitor session 2 source gigabitethernet0/1 rx
Switch(config)# monitor session 2 destination interface gigabitethernet0/2 encapsulation
replicate ingress dot1q vlan 6
Switch(config)# end
```

Specifying VLANs to Filter

Follow this procedure to limit SPAN source traffic to specific VLANs.

BEFORE YOU BEGIN

Review the "Information About SPAN and RSPAN" section on page 11-1 and "Guidelines and Limitations" section on page 11-8.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	Remove any existing SPAN configuration for the session. For *session_number*, the range is 1 to 66. Specify **all** to remove all SPAN sessions, **local** to remove all local sessions, or **remote** to remove all remote SPAN sessions.
Step 3	**monitor session** *session_number* **source interface** *interface-id*	Specify the characteristics of the source port (monitored port) and SPAN session. For *session_number*, the range is 1 to 66. For *interface-id*, specify the source port to monitor. The interface specified must already be configured as a trunk port.
Step 4	**monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**]	Limit the SPAN source traffic to specific VLANs. For *session_number*, enter the session number specified in Step 3. For *vlan-id*, the range is 1 to 4094. (Optional) Use a comma (**,**) to specify a series of VLANs, or use a hyphen (**-**) to specify a range of VLANs. Enter a space before and after the comma; enter a space before and after the hyphen.

	Command	Purpose
Step 5	**monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation** {**dot1q** | **replicate**}]}	Specify the SPAN session and the destination port (monitoring port). For *session_number*, specify the session number entered in Step 3. For *interface-id*, specify the destination port. The destination interface must be a physical port; it cannot be an EtherChannel, and it cannot be a VLAN. (Optional) [**,** | **-**] Specify a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen. (Optional) Enter **encapsulation dot1q** or **encapsulation replicate** to specify 802.1Q encapsulation or that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged).
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show monitor** [**session** *session_number*] **show running-config**	Verify the configuration.
Step 8	**copy running-config startup-config**	(Optional) Save the configuration in the configuration file.

To monitor all VLANs on the trunk port, use the **no monitor session** *session_number* **filter** global configuration command.

EXAMPLE

This example shows how to remove any existing configuration on SPAN session 2, configure SPAN session 2 to monitor traffic received on Gigabit Ethernet trunk port 2, and send traffic for only VLANs 1 through 5 and VLAN 9 to destination Gigabit Ethernet port 1:

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet0/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5 , 9
Switch(config)# monitor session 2 destination interface gigabitethernet0/1
Switch(config)# end
```

Configuring RSPAN

Configuring a VLAN as an RSPAN VLAN

Create a new VLAN to be the RSPAN VLAN for the RSPAN session. You must create the RSPAN VLAN in all switches that will participate in RSPAN. You must configure RSPAN VLAN on source and destination switches and any intermediate switches.

To get an efficient flow of RSPAN traffic, manually delete the RSPAN VLAN from all trunks that do not need to carry the RSPAN traffic.

BEFORE YOU BEGIN

Review the "Information About SPAN and RSPAN" section on page 11-1 and "Guidelines and Limitations" section on page 11-8.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vlan** *vlan-id*	Enter a VLAN ID to create a VLAN, or enter the VLAN ID of an existing VLAN, and enter VLAN configuration mode. The range is 2 to 1001 and 1006 to 4094. **Note** The RSPAN VLAN cannot be VLAN 1 (the default VLAN) or VLAN IDs 1002 through 1005 (reserved for Token Ring and FDDI VLANs). If you enter the VLAN ID of a UNI-ENI community VLAN, you must remove the community VLAN type by entering the **no uni-vlan** VLAN configuration command.
Step 3	**remote-span**	Configure the VLAN as an RSPAN VLAN.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save the configuration in the configuration file.

To remove the remote SPAN characteristic from a VLAN and convert it back to a UNI-ENI isolated VLAN, use the **no remote-span** VLAN configuration command.

EXAMPLE

This example shows how to create RSPAN VLAN 901:

```
Switch(config)# vlan 901
Switch(config-vlan)# remote span
Switch(config-vlan)# end
```

Creating an RSPAN Source Session

Follow this procedure to start an RSPAN source session and to specify the monitored source and the destination RSPAN VLAN.

BEFORE YOU BEGIN

Review the "Information About SPAN and RSPAN" section on page 11-1 and "Guidelines and Limitations" section on page 11-8.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	Remove any existing RSPAN configuration for the session. For *session_number*, the range is 1 to 66. Specify **all** to remove all RSPAN sessions, **local** to remove all local sessions, or **remote** to remove all remote SPAN sessions.
Step 3	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]	Specify the RSPAN session and the source port (monitored port). For *session_number*, the range is 1 to 66. Enter a source port or source VLAN for the RSPAN session: • For *interface-id*, specify the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (**port-channel** *port-channel-number*). *Valid port-channel numbers are 1 to 48.* • For *vlan-id*, specify the source VLAN to monitor. The range is 1 to 4094 (excluding the RSPAN VLAN). **Note** A single session can include multiple sources (ports or VLANs), defined in a series of commands, but you cannot combine source ports and source VLANs in one session. (Optional) [**,** | **-**] Specify a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen. (Optional) Specify the direction of traffic to monitor. If you do not specify a traffic direction, the source interface sends both sent and received traffic. • **both**—Monitor both received and sent traffic. • **rx**—Monitor received traffic. • **tx**—Monitor sent traffic.
Step 4	**monitor session** *session_number* **destination remote vlan** *vlan-id*	Specify the RSPAN session and the destination RSPAN VLAN. For *session_number*, enter the number defined in Step 3. For *vlan-id*, specify the source RSPAN VLAN to monitor.
Step 5	**end**	Return to privileged EXEC mode.

	Command	Purpose
Step 6	**show monitor** [**session** *session_number*] **show running-config**	Verify the configuration.
Step 7	**copy running-config startup-config**	(Optional) Save the configuration in the configuration file.

To delete a SPAN session, use the **no monitor session** *session_number* global configuration command.

To remove a source port or VLAN from the SPAN session, use the **no monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} global configuration command. To remove the RSPAN VLAN from the session, use the **no monitor session** *session_number* **destination remote vlan** *vlan-id.*

EXAMPLE

This example shows how to remove any existing RSPAN configuration for session 1, configure RSPAN session 1 to monitor multiple source interfaces, and configure the destination as RSPAN VLAN 901:

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet0/1 tx
Switch(config)# monitor session 1 source interface gigabitethernet0/2 rx
Switch(config)# monitor session 1 source interface port-channel 12
Switch(config)# monitor session 1 destination remote vlan 901
Switch(config)# end
```

Creating an RSPAN Destination Session

You configure the RSPAN destination session on a different switch; that is, not the switch on which the source session was configured. Follow this procedure to define the RSPAN VLAN on that switch, to create an RSPAN destination session, and to specify the source RSPAN VLAN and the destination port.

BEFORE YOU BEGIN

Review the "Information About SPAN and RSPAN" section on page 11-1 and "Guidelines and Limitations" section on page 11-8.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vlan** *vlan-id*	Enter the VLAN ID of the RSPAN VLAN created from the source switch, and enter VLAN configuration mode. **Note** If the VLAN is configured as a UNI-ENI community VLAN, you must remove the community VLAN type by entering the **no uni-vlan** VLAN configuration command.
Step 3	**remote-span**	Identify the VLAN as the RSPAN VLAN.
Step 4	**exit**	Return to global configuration mode.

	Command	Purpose
Step 5	**no monitor session** {*session_number* | **all** | **local** | **remote**}	Remove any existing RSPAN configuration for the session. For *session_number*, the range is 1 to 66. Specify **all** to remove all RSPAN sessions, **local** to remove all local sessions, or **remote** to remove all remote SPAN sessions.
Step 6	**monitor session** *session_number* **source remote vlan** *vlan-id*	Specify the RSPAN session and the source RSPAN VLAN. For *session_number*, the range is 1 to 66. For *vlan-id*, specify the source RSPAN VLAN to monitor.
Step 7	**monitor session** *session_number* **destination interface** *interface-id*	Specify the RSPAN session and the destination interface. For *session_number*, enter the number defined in Step 6. **Note** In an RSPAN destination session, you must use the same session number for the source RSPAN VLAN and the destination port. For *interface-id*, specify the destination interface. The destination interface must be a physical interface. **Note** Though visible in the command-line help string, **encapsulation replicate** is not supported for RSPAN. The original VLAN ID is overwritten by the RSPAN VLAN ID, and all packets appear on the destination port as untagged.
Step 8	**end**	Return to privileged EXEC mode.
Step 9	**show monitor** [**session** *session_number*] **show running-config**	Verify the configuration.
Step 10	**copy running-config startup-config**	(Optional) Save the configuration in the configuration file.

To delete a SPAN session, use the **no monitor session** *session_number* global configuration command. To remove a destination port from the SPAN session, use the **no monitor session** *session_number* **destination interface** *interface-id* global configuration command. To remove the RSPAN VLAN from the session, use the **no monitor session** *session_number* **source remote vlan** *vlan-id.*

EXAMPLE

This example shows how to configure VLAN 901 as the source remote VLAN and port 1 as the destination interface:

```
Switch(config)# monitor session 1 source remote vlan 901
Switch(config)# monitor session 1 destination interface gigabitethernet0/1
Switch(config)# end
```

Creating an RSPAN Destination Session and Configuring Ingress Traffic

Follow this procedure to create an RSPAN destination session, to specify the source RSPAN VLAN and the destination port, and to enable ingress traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance).

BEFORE YOU BEGIN

Configure the RSPAN VLAN as described in the "Creating an RSPAN Destination Session" section on page 11-20.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	Remove any existing SPAN configuration for the session.
Step 3	**monitor session** *session_number* **source remote vlan** *vlan-id*	Specify the RSPAN session and the source RSPAN VLAN. For *session_number*, the range is 1 to 66. For *vlan-id*, specify the source RSPAN VLAN to monitor.

	Command	Purpose
Step 4	**monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**ingress** {**dot1q vlan** *vlan-id* | **untagged vlan** *vlan-id* | **vlan** *vlan-id*}]}	Specify the SPAN session, the destination port, the packet encapsulation, and the ingress VLAN and encapsulation. For *session_number*, enter the number defined in Step 4. **Note** In an RSPAN destination session, you must use the same session number for the source RSPAN VLAN and the destination port. For *interface-id*, specify the destination interface. The destination interface must be a physical interface. **Note** Though visible in the command-line help string, **encapsulation replicate** is not supported for RSPAN. The original VLAN ID is overwritten by the RSPAN VLAN ID, and all packets appear on the destination port as untagged. (Optional) **[, | -]** Specify a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen. Enter **ingress** with additional keywords to enable ingress traffic forwarding on the destination port and to specify the encapsulation type: • **dot1q vlan** *vlan-id*—Forward incoming packets with 802.1Q encapsulation with the specified VLAN as the default VLAN. • **untagged vlan** *vlan-id* or **vlan** *vlan-id*—Forward incoming packets with untagged encapsulation type with the specified VLAN as the default VLAN.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show monitor** [**session** *session_number*] **show running-config**	Verify the configuration.
Step 7	**copy running-config startup-config**	(Optional) Save the configuration in the configuration file.

To delete an RSPAN session, use the **no monitor session** *session_number* global configuration command. To remove a destination port from the RSPAN session, use the **no monitor session** *session_number* **destination interface** *interface-id* global configuration command. The ingress options are ignored with the **no** form of the command.

EXAMPLE

This example shows how to configure VLAN 901 as the source remote VLAN in RSPAN session 2, configure Gigabit Ethernet source port 2 as the destination interface, and enable ingress forwarding on the interface with VLAN 6 as the default incoming VLAN:

```
Switch(config)# monitor session 2 source remote vlan 901
Switch(config)# monitor session 2 destination interface gigabitethernet0/2 ingress vlan 6
Switch(config)# end
```

Specifying VLANs to Filter

Follow this procedure to configure the RSPAN source session to limit RSPAN source traffic to specific VLANs.

BEFORE YOU BEGIN

Review the "Information About SPAN and RSPAN" section on page 11-1 and "Guidelines and Limitations" section on page 11-8.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no monitor session** {*session_number* | **all** | **local** | **remote**}	Remove any existing SPAN configuration for the session. For *session_number*, the range is 1 to 66. Specify **all** to remove all SPAN sessions, **local** to remove all local sessions, or **remote** to remove all remote SPAN sessions.
Step 3	**monitor session** *session_number* **source interface** *interface-id*	Specify the characteristics of the source port (monitored port) and SPAN session. For *session_number*, the range is 1 to 66. For *interface-id*, specify the source port to monitor. The interface specified must already be configured as a trunk port.
Step 4	**monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**]	Limit the SPAN source traffic to specific VLANs. For *session_number*, enter the session number specified in step 3. For *vlan-id*, the range is 1 to 4094. (Optional) Use a comma (**,**) to specify a series of VLANs or use a hyphen (**-**) to specify a range of VLANs. Enter a space before and after the comma; enter a space before and after the hyphen.
Step 5	**monitor session** *session_number* **destination remote vlan** *vlan-id*	Specify the RSPAN session and the destination remote VLAN (RSPAN VLAN). For *session_number*, enter the session number specified in step 3. For *vlan-id*, specify the RSPAN VLAN to carry the monitored traffic to the destination port.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show monitor** [**session** *session_number*] **show running-config**	Verify the configuration.
Step 8	**copy running-config startup-config**	(Optional) Save the configuration in the configuration file.

To monitor all VLANs on the trunk port, use the **no monitor session** *session_number* **filter vlan** global configuration command.

EXAMPLE

This example shows how to remove any existing configuration on RSPAN session 2, configure RSPAN session 2 to monitor traffic received on trunk port 2, and send traffic for only VLANs 2 through 5 and 9 to destination RSPAN VLAN 902:

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet0/2 rx
Switch(config)# monitor session 2 filter vlan 2 - 5 , 9
Switch(config)# monitor session 2 destination remote vlan 902
Switch(config)# end
```

Verifying Configuration

To display the current SPAN or RSPAN configuration, use the **show monitor** user EXEC command. You can also use the **show running-config** privileged EXEC command to display configured SPAN or RSPAN sessions.

Configuration Example

This example shows how to set up SPAN session 1 for monitoring source port traffic to a destination port. First, any existing SPAN configuration for session 1 is deleted, and then bidirectional traffic is mirrored from source Gigabit Ethernet port 1 to destination Gigabit Ethernet port 2, retaining the encapsulation method.

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet0/1
Switch(config)# monitor session 1 destination interface gigabitethernet0/2
encapsulation replicate
Switch(config)# end
```

This example shows how to remove port 1 as a SPAN source for SPAN session 1:

```
Switch(config)# no monitor session 1 source interface gigabitethernet0/1
Switch(config)# end
```

This example shows how to disable received traffic monitoring on port 1, which was configured for bidirectional monitoring:

```
Switch(config)# no monitor session 1 source interface gigabitethernet0/1 rx
```

The monitoring of traffic received on port 1 is disabled, but traffic sent from this port continues to be monitored.

This example shows how to remove any existing configuration on SPAN session 2, configure SPAN session 2 to monitor received traffic on all ports belonging to VLANs 1 through 3, and send it to destination Gigabit Ethernet port 2. The configuration is then modified to also monitor all traffic on all ports belonging to VLAN 10.

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source vlan 1 - 3 rx
Switch(config)# monitor session 2 destination interface gigabitethernet0/2
Switch(config)# monitor session 2 source vlan 10
Switch(config)# end
```

This example shows how to remove any existing configuration on SPAN session 2, configure SPAN session 2 to monitor sent traffic on Gigabit Ethernet source port 1, send it to destination Gigabit Ethernet port 2 with the same egress encapsulation type as the source port, and enable incoming forwarding with 802.1Q encapsulation and VLAN 6 as the default ingress VLAN:

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source gigabitethernet0/1 rx
Switch(config)# monitor session 2 destination interface gigabitethernet0/2 encapsulation
replicate ingress dot1q vlan 6
Switch(config)# end
```

This example shows how to remove any existing configuration on SPAN session 2, configure SPAN session 2 to monitor traffic received on Gigabit Ethernet trunk port 2, and send traffic for only VLANs 1 through 5 and VLAN 9 to destination Gigabit Ethernet port 1:

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet0/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5 , 9
Switch(config)# monitor session 2 destination interface gigabitethernet0/1
Switch(config)# end
```

This example shows how to create RSPAN VLAN 901:

```
Switch(config)# vlan 901
Switch(config-vlan)# remote span
Switch(config-vlan)# end
```

This example shows how to remove any existing RSPAN configuration for session 1, configure RSPAN session 1 to monitor multiple source interfaces, and configure the destination as RSPAN VLAN 901:

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet0/1 tx
Switch(config)# monitor session 1 source interface gigabitethernet0/2 rx
Switch(config)# monitor session 1 source interface port-channel 12
Switch(config)# monitor session 1 destination remote vlan 901
Switch(config)# end
```

This example shows how to configure VLAN 901 as the source remote VLAN and port 1 as the destination interface:

```
Switch(config)# monitor session 1 source remote vlan 901
Switch(config)# monitor session 1 destination interface gigabitethernet0/1
Switch(config)# end
```

This example shows how to remove any existing configuration on RSPAN session 2, configure RSPAN session 2 to monitor traffic received on trunk port 2, and send traffic for only VLANs 2 through 5 and 9 to destination RSPAN VLAN 902:

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet0/2 rx
Switch(config)# monitor session 2 filter vlan 2 - 5 , 9
Switch(config)# monitor session 2 destination remote vlan 902
Switch(config)# end
```

Related Documents

- Cisco IOS Master Command List, All Releases

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

Configuring RMON

This chapter describes how to configure Remote Network Monitoring (RMON) on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*.

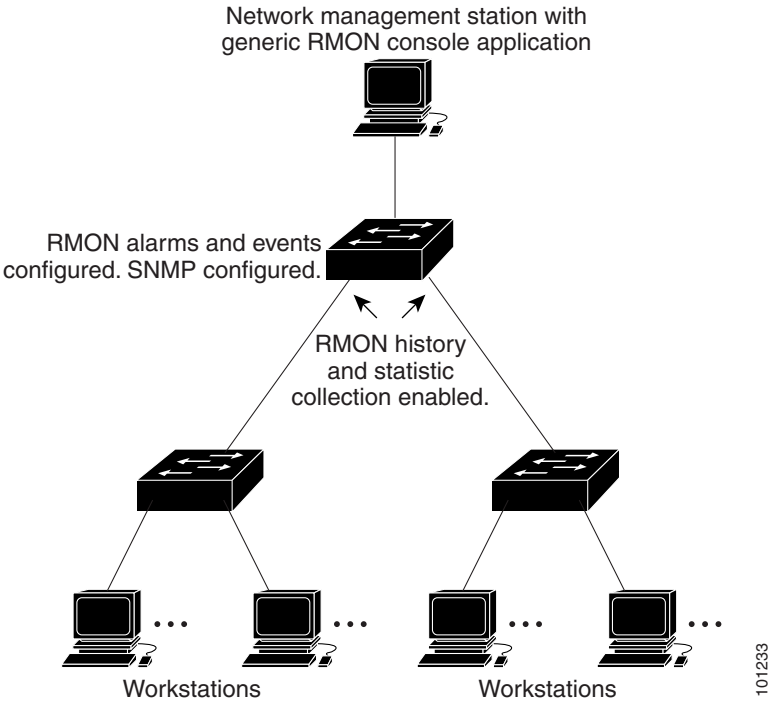
RMON is a standard monitoring specification that defines a set of statistics and functions that can be exchanged between RMON-compliant console systems and network probes. RMON provides you with comprehensive network-fault diagnosis, planning, and performance-tuning information.

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 12-8.

Information About RMON

RMON is an Internet Engineering Task Force (IETF) standard monitoring specification that allows various network agents and console systems to exchange network monitoring data. You can use the RMON feature with the Simple Network Management Protocol (SNMP) agent in the switch to monitor all the traffic flowing among switches on all connected LAN segments as shown in Figure 12-1.

Figure 12-1 Remote Monitoring Example



The switch supports these RMON groups (defined in RFC 1757):

- Statistics (RMON group 1)—Collects Ethernet statistics (including Fast Ethernet and Gigabit Ethernet statistics, depending on the switch type and supported interfaces) on an interface.
- History (RMON group 2)—Collects a history group of statistics on Ethernet ports (including Fast Ethernet and Gigabit Ethernet statistics, depending on the switch type and supported interfaces) for a specified polling interval.
- Alarm (RMON group 3)—Monitors a specific management information base (MIB) object for a specified interval, triggers an alarm at a specified value (rising threshold), and resets the alarm at another value (falling threshold). Alarms can be used with events; the alarm triggers an event, which can generate a log entry or an SNMP trap.
- Event (RMON group 9)—Specifies the action to take when an event is triggered by an alarm. The action can be to generate a log entry or an SNMP trap.

Because switches supported by this software release use hardware counters for RMON data processing, the monitoring is more efficient, and little processing power is required.

Note 64-bit counters are not supported for RMON alarms.

Prerequisites

You must also configure SNMP on the switch to access RMON MIB objects. For more information, see Chapter 14, “Configuring SNMP.”

Guidelines and Limitations

64-bit counters are not supported for RMON alarms.

Default Settings

RMON is disabled by default; no alarms or events are configured.

Configuring RMON

- Configuring RMON Alarms and Events, page 12-3 (required)
- Collecting Group History Statistics on an Interface, page 12-5 (optional)
- Collecting Group Ethernet Statistics on an Interface, page 12-6 (optional)

Configuring RMON Alarms and Events

You can configure your switch for RMON by using the command-line interface (CLI) or an SNMP-compatible network management station. We recommend that you use a generic RMON console application on the network management station (NMS) to take advantage of the RMON network management capabilities.

BEFORE YOU BEGIN

To learn more about alarms and events and how they interact with each other, see RFC 1757.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**rmon alarm** *number variable interval* {**absolute** | **delta**} **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *string*]	Set an alarm on a MIB object. • For *number*, specify the alarm number. The range is 1 to 65535. • For *variable*, specify the MIB object to monitor. • For *interval*, specify the time in seconds the alarm monitors the MIB variable. The range is 1 to 4294967295 seconds. • Specify the **absolute** keyword to test each MIB variable directly. Specify the **delta** keyword to test the change between samples of a MIB variable. • For *value*, specify a number at which the alarm is triggered and one for when the alarm is reset. The range for the rising threshold and falling threshold values is -2147483648 to 2147483647. • (Optional) For *event-number*, specify the event number to trigger when the rising or falling threshold exceeds its limit. • (Optional) For **owner** *string*, specify the owner of the alarm.
Step 3	**rmon event** *number* [**description** *string*] [**log**] [**owner** *string*] [**trap** *community*]	Add an event in the RMON event table that is associated with an RMON event number. • For *number*, assign an event number. The range is 1 to 65535. • (Optional) For **description** *string*, specify a description of the event. • (Optional) Use the **log** keyword to generate an RMON log entry when the event is triggered. • (Optional) For **owner** *string*, specify the owner of this event. • (Optional) For **trap** *community*, enter the SNMP community string used for this trap.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable an alarm, use the **no rmon alarm** *number* global configuration command on each alarm you configured. You cannot disable at once all the alarms that you configured. To disable an event, use the **no rmon event** *number* global configuration command.

EXAMPLE

You can set an alarm on any MIB object. The following example configures RMON alarm number 10 by using the **rmon alarm** command. The alarm monitors the MIB variable *ifEntry.20.1* once every 20 seconds until the alarm is disabled and checks the change in the variable's rise or fall. If the *ifEntry.20.1* value shows a MIB counter increase of 15 or more, such as from 100000 to 100015, the alarm is triggered. The alarm in turn triggers event number 1, which is configured with the **rmon event** command. Possible events can include a log entry or an SNMP trap. If the *ifEntry.20.1* value changes by 0, the alarm is reset and can be triggered again.

```
Switch(config)# rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1
falling-threshold 0 owner jjohnson
```

The following example creates RMON event number 1 by using the **rmon event** command. The event is defined as *High ifOutErrors* and generates a log entry when the event is triggered by the alarm. The user *jjones* owns the row that is created in the event table by this command. This example also generates an SNMP trap when the event is triggered.

```
Switch(config)# rmon event 1 log trap eventtrap description "High ifOutErrors" owner
jjones
```

Collecting Group History Statistics on an Interface

BEFORE YOU BEGIN

You must first configure RMON alarms and events to display collection information.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface on which to collect history, and enter interface configuration mode.
Step 3	**no shutdown**	Enable the port, if necessary. By default, user network node interfaces (UNIs) and enhanced network interfaces (ENIs) are disabled, and network node interfaces (NNIs) are enabled.

	Command	Purpose
Step 4	**rmon collection history** *index* [**buckets** *bucket-number*] [**interval** *seconds*] [**owner** *ownername*]	Enable history collection for the specified number of buckets and time period. • For *index*, identify the RMON group of statistics The range is 1 to 65535. • (Optional) For **buckets** *bucket-number,* specify the maximum number of buckets desired for the RMON collection history group of statistics. The range is 1 to 65535. The default is 50 buckets. • (Optional) For **interval** *seconds*, specify the number of seconds in each polling cycle. The range is 1 to 3600. The default is 1800 seconds. • (Optional) For **owner** *ownername*, enter the name of the owner of the RMON group of statistics.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config**	Verify your entries.
Step 7	**show rmon history**	Display the contents of the switch history table.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable history collection, use the **no rmon collection history** *index* interface configuration command.

EXAMPLE

The following example shows how to enable an RMON MIB collection history group of statistics with an ID number of 20 and an owner as john:

```
Switch(config-if)# rmon collection history controlEntry 20 owner john
```

Collecting Group Ethernet Statistics on an Interface

BEFORE YOU BEGIN

You must first configure RMON alarms and events to display collection information.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface on which to collect statistics, and enter interface configuration mode.
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.

	Command	Purpose
Step 4	**rmon collection stats** *index* [**owner** *ownername*]	Enable RMON statistic collection on the interface. • For *index*, specify the RMON group of statistics. The range is from 1 to 65535. • (Optional) For **owner** *ownername*, enter the name of the owner of the RMON group of statistics.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config**	Verify your entries.
Step 7	**show rmon statistics**	Display the contents of the switch statistics table.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable the collection of group Ethernet statistics, use the **no rmon collection stats** *index* interface configuration command.

EXAMPLE

This example shows how to collect RMON statistics for the owner *root*:

```
Switch(config)# interface fastethernet0/1
Switch(config)# no shutdown
Switch(config-if)# rmon collection stats 2 owner root
```

Verifying Configuration

Command	Purpose
show rmon	Displays general RMON statistics.
show rmon alarms	Displays the RMON alarm table.
show rmon events	Displays the RMON event table.
show rmon history	Displays the RMON history table.
show rmon statistics	Displays the RMON statistics table.

Configuration Example

The following example creates RMON event number 1 by using the **rmon event** command. The event is defined as *High ifOutErrors* and generates a log entry when the event is triggered by the alarm. The user *jjones* owns the row that is created in the event table by this command. This example also generates an SNMP trap when the event is triggered.

```
Switch(config)# rmon event 1 log trap eventtrap description "High ifOutErrors" owner
jjones
```

The following example shows how to enable an RMON MIB collection history group of statistics with an ID number of 20 and an owner as john:

```
Switch(config-if)# rmon collection history controlEntry 20 owner john
```

This example shows how to collect RMON statistics for the owner *root*:

```
Switch(config)# interface fastethernet0/1
Switch(config)# no shutdown
Switch(config-if)# rmon collection stats 2 owner root
```

Related Documents

- RMON Command Reference
- Cisco IOS Configuration Fundamentals Command Reference

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

Configuring System Message Logging

This chapter describes how to configure system message logging on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*.

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 13-17.

This chapter consists of these sections:

Information About 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, Cisco System Messages.

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.

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 13-1 describes the elements of syslog messages.

Table 13-1 System Log Message Elements

Element	Description
seq no:	Stamps log messages with a sequence number only if the **service sequence-numbers** global configuration command is configured. For more information, see the "Enabling and Disabling Sequence Numbers in Log Messages" section on page 13-9.
timestamp formats: *mm/dd hh:mm:ss* or *hh:mm:ss* (short uptime) or *d h* (long uptime)	Date and time of the message or event. This information appears only if the **service timestamps log** [**datetime** | **log**] global configuration command is configured. For more information, see the "Enabling and Disabling Time Stamps on Log Messages" section on page 13-8.
facility	The facility to which the message refers (for example, SNMP, SYS, and so forth). For a list of supported facilities, see Table 13-3 on page 13-15.
severity	Single-digit code from 0 to 7 that is the severity of the message. For a description of the severity levels, see Table 13-2 on page 13-10.
MNEMONIC	Text string that uniquely describes the message.
description	Text string containing detailed information about the event being reported.

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
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to down 2
```

```
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
*Mar  1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

Prerequisites

Review the "Information About System Message Logging" section on page 13-1.

Guidelines and Limitations

Caution Logging messages to the console at a high rate can cause high CPU utilization and adversely affect how the switch operates.

Default Settings

Feature	Default Setting
System message logging to the console	Enabled.
Console severity	Debugging (and numerically lower levels; see Table 13-2 on page 13-10).
Logging file configuration	No filename specified.
Logging buffer size	4096 bytes.
Logging history size	1 message.
Time stamps	Disabled.
Synchronous logging	Disabled.
Logging server	Disabled.
Syslog server IP address	None configured.
Server facility	Local7 (see Table 13-3 on page 13-15).
Server severity	Informational (and numerically lower levels; see Table 13-2 on page 13-10).

Configuring System Message Logging

- Disabling Message Logging, page 13-4 (optional)
- Setting the Message Display Destination Device, page 13-5 (optional)
- Synchronizing Log Messages, page 13-6 (optional)
- Enabling and Disabling Time Stamps on Log Messages, page 13-8 (optional)
- Enabling and Disabling Sequence Numbers in Log Messages, page 13-9 (optional)

- Defining the Message Severity Level, page 13-9 (optional)
- Limiting Syslog Messages Sent to the History Table and to SNMP, page 13-11 (optional)
- Enabling the Configuration-Change Logger, page 13-13 (optional)
- Configuring UNIX Syslog Servers, page 13-14 (optional)

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.

BEFORE YOU BEGIN

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 13-6.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no logging console**	Disable message logging.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config** or **show logging**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To re-enable message logging after it has been disabled, use the **logging on** global configuration command.

EXAMPLE

```
Switch(config)# no logging console
Switch(config)# end
```

Setting the Message Display Destination Device

If message logging is enabled, you can send messages to specific locations in addition to the console.

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.

BEFORE YOU BEGIN

If message logging is disabled, use the **logging on** global configuration command to re-enable it.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**logging buffered** [*size*]	Log messages to an internal buffer on the switch. The default buffer size is 4096. The range is 4096 to 2147483647 bytes. If the switch fails, the log file is lost unless you previously saved it to Flash memory. See Step 4. **Note** Do not make the buffer size too large because the switch could run out of memory for other tasks. Use the **show memory** privileged EXEC command to view the free processor memory on the switch. However, this value is the maximum available, and the buffer size should *not* be set to this amount.
Step 3	**logging** *host*	Log messages to a UNIX syslog server host. For *host*, specify the name or IP address of the host to be used as the syslog server. To build a list of syslog servers that receive logging messages, enter this command more than once. For complete syslog server configuration steps, see the "Configuring UNIX Syslog Servers" section on page 13-14.

	Command	Purpose
Step 4	**logging file flash:***filename* [*max-file-size* [*min-file-size*]] [*severity-level-number* | *type*]	Store log messages in a file in flash memory. • For *filename*, enter the log message filename. • (Optional) For *max-file-size, s*pecify the maximum logging file size. The range is 4096 to 2147483647. The default is 4096 bytes. • (Optional) For *min-file-size, s*pecify the minimum logging file size. The range is 1024 to 2147483647. The default is 2048 bytes. • (Optional) For *severity-level-number* | *type,* specify either the logging severity level or the logging type. The severity range is 0 to 7. For a list of logging type keywords, see Table 13-2 on page 13-10. By default, the log file receives debugging messages and numerically lower levels.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**terminal monitor**	Log messages to a nonconsole terminal during the current session. Terminal parameter-setting commands are set locally and do not remain in effect after the session has ended. You must perform this step for each session to see the debugging messages.
Step 7	**show running-config**	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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.

EXAMPLE

The following example shows how to enable standard system logging to the local syslog buffer:

```
Switch(config)# logging buffered
```

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.

BEFORE YOU BEGIN

Caution By configuring abnormally large message queue limits and setting the terminal to "terminal monitor" on a terminal that is accessible to intruders, you expose yourself to "denial of service" attacks. An intruder could carry out the attack by putting the terminal in synchronous output mode, making a Telnet connection to a remote host, and leaving the connection idle. This could cause large numbers of messages to be generated and queued, and these messages could consume all available RAM. You should guard against this type of attack through proper configuration.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
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.

	Command	Purpose
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable synchronization of unsolicited messages and debug output, use the **no logging synchronous** [**level** *severity-level* | **all**] [**limit** *number-of-buffers*] line configuration command.

EXAMPLE

In the following example, synchronous logging for line 4 is enabled with a severity level of 6. Then synchronous logging for line 2 is enabled with a severity level of 7 and is specified with a maximum number of buffer lines of 1,000.

```
Switch(config)# line 4
Switch(config-line)# logging synchronous level 6
Switch(config-line)# exit
Switch(config)# line 2
Switch(config-line)# logging synchronous level 7 limit 1000
Switch(config-line)# end
```

Enabling and Disabling Time Stamps on Log Messages

By default, log messages are not time stamped.

BEFORE YOU BEGIN

Ensure that the system clock is set correctly. For more information, see Chapter 4, "Administering the Switch."

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**service timestamps log uptime** or **service timestamps log datetime** [**msec**] [**localtime**] [**show-timezone**]	Enable log time stamps. The first command enables time stamps on log messages, showing the time since the system was rebooted. 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.
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.

EXAMPLE

This example shows part of a logging display with the **service timestamps log datetime** global configuration command enabled:

```
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

This example shows part of a logging display with the s**ervice timestamps log uptime** global configuration command enabled:

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

Enabling and Disabling Sequence Numbers in Log Messages

Because there is a chance that more than one log message can have the same 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.

BEFORE YOU BEGIN

Review the "Information About System Message Logging" section on page 13-1.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**service sequence-numbers**	Enable sequence numbers.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable sequence numbers, use the **no service sequence-numbers** global configuration command.

EXAMPLE

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. Table 13-2 describes the *level* keywords. It also lists the corresponding UNIX syslog definitions from the most severe level to the least severe level.

Table 13-2 Message Logging Level Keywords

Level Keyword	Level	Description	Syslog Definition
emergencies	0	System unstable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

The software generates four other categories of messages:

- Error messages about software or hardware malfunctions, displayed at levels **warnings** through **emergencies**. These types of messages mean that the functionality of the 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.

BEFORE YOU BEGIN

Caution The console is a slow display device. In message storms some logging messages may be silently dropped when the console queue becomes full. Set severity levels accordingly.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**logging console** *level*	Limit messages logged to the console. By default, the console receives debugging messages and numerically lower levels (see Table 13-2 on page 13-10).
Step 3	**logging monitor** *level*	Limit messages logged to the terminal lines. By default, the terminal receives debugging messages and numerically lower levels (see Table 13-2 on page 13-10).

	Command	Purpose
Step 4	**logging trap** *level*	Limit messages logged to the syslog servers. By default, syslog servers receive informational messages and numerically lower levels (see Table 13-2 on page 13-10). For complete syslog server configuration steps, see the "Configuring UNIX Syslog Servers" section on page 13-14.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config** or **show logging**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Note Specifying a *level* causes messages at that level and numerically lower levels to 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.

EXAMPLE

The following example shows how to change the level of messages sent to the console terminal to alerts, meaning that messages at levels 0 and 1 are sent:

```
Switch(config)# logging console alerts
```

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 13-2 on page 13-10) are stored in the history table even if syslog traps are not enabled.

BEFORE YOU BEGIN

For information about enabling syslog message traps using the **snmp-server enable trap** command, see Chapter 14, "Configuring SNMP."

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**logging history** *level*[1]	Change the default level of syslog messages stored in the history file and sent to the SNMP server. See Table 13-2 on page 13-10 for a list of *level* keywords. By default, **warnings**, **errors**, **critical**, **alerts**, and **emergencies** messages are sent.
Step 3	**logging history size** *number*	Specify the number of syslog messages that can be stored in the history table. The default is to store one message. The range is 0 to 500 messages.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

1. Table 13-2 lists the level keywords and severity level. For SNMP usage, the severity level values increase by 1. For example, emergencies equal 1, not 0, and critical equals 3, not 2.

When the history table is full (it contains the maximum number of message entries specified with the **logging history size** global configuration command), the oldest message entry is deleted from the table to allow the new message entry to be stored.

To return the logging of syslog messages to the default level, use the **no logging history** global configuration command. To return the number of messages in the history table to the default value, use the **no logging history size** global configuration command.

EXAMPLE

In the following example, the logging history 1 command is used to configure the system to save only level 1 (alert) and level 0 (emergency) messages to the logging history table, and, by extension, to send only these levels in the SNMP notifications. The configuration is then confirmed using the show logging history command.

```
Switch(config)# logging history 1
Switch(config)# snmp-server enable traps syslog
Switch(config)# end
Switch#
4w0d: %SYS-5-CONFIG_I: Configured from console by console
Switch# show logging history
Syslog History Table:1 maximum table entries,
! The following line indicates that 'logging history level 1' (alerts) is configured.
saving level alerts or higher
 18 messages ignored, 0 dropped, 0 recursion drops
 1 table entries flushed
 SNMP notifications enabled, 0 notifications sent
   entry number 2 : LINK-3-UPDOWN
    Interface FastEthernet0, changed state to up
    timestamp: 2766
Switch#
```

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.

BEFORE YOU BEGIN

If you disable configuration logging, all configuration log records that were collected are purged.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**archive**	Enter archive configuration mode.
Step 3	**log config**	Enter configuration-change logger configuration mode.
Step 4	**logging enable**	Enable configuration change logging.
Step 5	**logging size** *entries*	(Optional) Configure the number of entries retained in the configuration log. The range is from 1 to 1000. The default is 100. **Note** When the configuration log is full, the oldest log entry is removed each time a new entry is entered.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show archive log config**	Verify your entries by viewing the configuration log.

EXAMPLE

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.

BEFORE YOU BEGIN

Some recent versions of UNIX syslog daemons no longer accept by default syslog packets from the network. If this is the case with your system, use the UNIX **man syslogd** command to decide what options must be added to or removed from the syslog command line to enable logging of remote syslog messages.

DETAILED STEPS

Step 1 Log in as root.

Step 2 Add a line such as the following to the file /etc/syslog.conf:

local7.debug /usr/adm/logs/*cisco.log*

The **local7** keyword specifies the logging facility to be used; see Table 13-3 on page 13-15 for information on the facilities. The **debug** keyword specifies the syslog level; see Table 13-2 on page 13-10 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 3 Create the log file by entering these commands at the UNIX shell prompt:

```
$ touch /var/log/cisco.log
$ chmod 666 /var/log/cisco.log
```

Step 4 Make sure the syslog daemon reads the new changes:

```
$ kill -HUP `cat /etc/syslog.pid`
```

For more information, see the **man syslog.conf** and **man syslogd** commands on your UNIX system.

Configuring the UNIX System Logging Facility

When sending system log messages to an external device, you can cause the switch to identify its messages as originating from any of the UNIX syslog facilities.

Table 13-3 lists the UNIX system facilities supported by the software.

Table 13-3 Logging Facility-Type Keywords

Facility Type Keyword	Description
auth	Authorization system
cron	Cron facility
daemon	System daemon
kern	Kernel
local0-7	Locally defined messages
lpr	Line printer system
mail	Mail system
news	USENET news
sys9-14	System use
syslog	System log
user	User process
uucp	UNIX-to-UNIX copy system

BEFORE YOU BEGIN

For more information about the UNIX system facilities, consult the operator's manual for your UNIX operating system.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**logging** *host*	Log messages to a UNIX syslog server host by entering its IP address. To build a list of syslog servers that receive logging messages, enter this command more than once.
Step 3	**logging trap** *level*	Limit messages logged to the syslog servers. Be default, syslog servers receive informational messages and lower. See Table 13-2 on page 13-10 for *level* keywords.
Step 4	**logging facility** *facility-type*	Configure the syslog facility. See Table 13-3 on page 13-15 for *facility-type* keywords. The default is **local7**.
Step 5	**end**	Return to privileged EXEC mode.

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

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.

EXAMPLE

In the following example, the user configures the syslog facility to the kernel facility type:

```
Switch(config)# logging facility kern
```

Verifying the Configuration

To display the logging configuration and the contents of the log buffer, use the **show logging** privileged EXEC command. For information about the fields in this display, see the *Cisco IOS Configuration Fundamentals Command Reference, Release 15.2M&T*.

Configuration Example

The following example shows how to enable standard system logging to the local syslog buffer:

```
Switch(config)# logging buffered
```

In the following example, synchronous logging for line 4 is enabled with a severity level of 6. Then synchronous logging for line 2 is enabled with a severity level of 7 and is specified with a maximum number of buffer lines of 1,000.

```
Switch(config)# line 4
Switch(config-line)# logging synchronous level 6
Switch(config-line)# exit
Switch(config)# line 2
Switch(config-line)# logging synchronous level 7 limit 1000
Switch(config-line)# end
```

This example shows part of a logging display with the **service timestamps log datetime** global configuration command enabled:

```
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

This example shows part of a logging display with the s**ervice timestamps log uptime** global configuration command enabled:

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

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)
```

The following example shows how to change the level of messages sent to the console terminal to alerts, meaning that messages at levels 0 and 1 are sent:

```
Switch(config)# logging console alerts
```

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
```

In the following example, the **logging history 1** command is used to configure the system to save only level 1 (alert) and level 0 (emergency) messages to the logging history table, and, by extension, to send only these levels in the SNMP notifications. The configuration is then confirmed using the **show logging history** command.

```
Switch(config)# logging history 1
Switch(config)# snmp-server enable traps syslog
Switch(config)# end
Switch#
4w0d: %SYS-5-CONFIG_I: Configured from console by console
Switch# show logging history
Syslog History Table:1 maximum table entries,
! The following line indicates that 'logging history level 1' (alerts) is configured.
saving level alerts or higher
 18 messages ignored, 0 dropped, 0 recursion drops
 1 table entries flushed
 SNMP notifications enabled, 0 notifications sent
   entry number 2 : LINK-3-UPDOWN
    Interface FastEthernet0, changed state to up
    timestamp: 2766
Switch#
```

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
```

Related Documents

- Cisco IOS Configuration Fundamentals Command Reference, Release 15.2M&T
- Cisco IOS Master Command List, All Releases
- Cisco System Messages

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

Configuring SNMP

This chapter describes how to configure the Simple Network Management Protocol (SNMP) on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*.

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 14-25. For commands for MIB bulk statistics data collection and process MIB configuration, see the Cisco IOS Master Command List, All Releases.

Information About 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. You can also configure a Cisco Process MIB CPU threshold table.

This section includes the following topics:

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 14-1 identifies the characteristics of the different combinations of security models and levels.

Table 14-1 SNMP Security Models and Levels

Model	Level	Authentication	Encryption	Result
SNMPv1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv2C	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
SNMPv3	noAuthNoPriv	Username	No	Uses a username match for authentication.
SNMPv3	authNoPriv	Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
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 14-2.

Table 14-2 SNMP Operations

Operation	Description
get-request	Retrieves a value from a specific variable.
get-next-request	Retrieves a value from a variable within a table.[1]

Table 14-2 SNMP Operations (continued)

Operation	Description
get-bulk-request[2]	Retrieves large blocks of data, such as multiple rows in a table, that would otherwise require the transmission of many small blocks of data.
get-response	Replies to a get-request, get-next-request, and set-request sent by an NMS.
set-request	Stores a value in a specific variable.
trap	An unsolicited message sent by an SNMP agent to an SNMP manager when some event has occurred.

1. With this operation, an SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.
2. The **get-bulk** command 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:

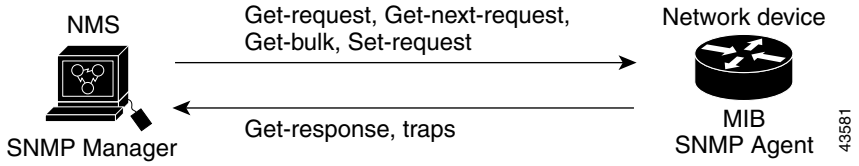
- Read-only (RO)—Gives read access to authorized management stations to all objects in the MIB except the community strings, but does not allow write access
- Read-write (RW)—Gives read and write access to authorized management stations to all objects in the MIB, but does not allow access to the community 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 14-1, 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 14-1 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 14-3 to assign an ifIndex value to an interface:

Table 14-3 ifIndex Values

Interface Type	ifIndex Range
SVI[1]	1–4999
EtherChannel	5000–5012
Loopback	5013–5077
Tunnel	5078–5142
Physical (such as Gigabit Ethernet or SFP[2]-module interfaces)	10000–14500
Null	14501

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 of MIB data from a device to a specified NMS, you group data from multiple MIBs into a 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.

Prerequisites

Review the "Information About SNMP" section on page 14-1 and "Guidelines and Limitations" section on page 14-7.

Guidelines and Limitations

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, Release 15.2M&T* 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.

Default Settings

Feature	Default Setting
SNMP agent	Disabled[1].
SNMP trap receiver	None configured.
SNMP traps	None enabled except the trap for TCP connections (**tty**).
SNMP version	If no **version** keyword is present, the default is Version 1.

Feature	Default Setting
SNMPv3 authentication	If no keyword is entered, the default is the **noauth** (noAuthNoPriv) security level.
SNMP notification type	If no type is specified, all notifications are sent.

1. This is the default at switch startup when the startup configuration does not have any **snmp-server** global configuration commands.

Configuring SNMP

Disabling the SNMP Agent

BEFORE YOU BEGIN

To determine whether the SNMP agent is enabled, use the **show startup-config** command. If the switch startup configuration has at least one **snmp-server** global configuration command, the SNMP agent is enabled.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no snmp-server**	Disable the SNMP agent operation.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

The **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.

EXAMPLE

The following example disables the current running version of SNMP:

```
Switch(config)# no snmp-server
```

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

BEFORE YOU BEGIN

- Obtain an established SNMP community string that defines the relationship between the SNMP manager and the agent.
- Obtain the IP address of the host defined to be the recipient of SNMP notifications.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**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.

	Command	Purpose
Step 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	(Optional) If you specified an IP standard access list number in Step 2, then create the list, repeating the command as many times as necessary. • For *access-list-number*, enter the access list number specified in Step 2. • The **deny** keyword denies access if the conditions are matched. The **permit** keyword permits access if the conditions are matched. • For *source*, enter the IP address of the SNMP managers that are permitted to use the community string to gain access to the agent. • (Optional) For *source-wildcard*, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore. Recall that the access list is always terminated by an implicit deny statement for everything.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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.

EXAMPLE

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.

BEFORE YOU BEGIN

Review the "Guidelines and Limitations" section on page 14-7.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**snmp-server engineID** {**local** *engineid-string* | **remote** *ip-address* [**udp-port** *port-number*] *engineid-string*}	Configure a name for either the local or remote copy of SNMP. • The *engineid-string* is a 24-character ID string with the name of the copy of SNMP. You need not specify the entire 24-character engine ID if it has trailing zeros. Specify only the portion of the engine ID up to the point where only zeros remain in the value. For example, to configure an engine ID of 123400000000000000000000, you can enter this: **snmp-server engineID local 1234** • If you select **remote**, specify the *ip-address* of the device that contains the remote copy of SNMP and the optional User Datagram Protocol (UDP) port to use for storing data on the remote device. The default is 162.

	Command	Purpose
Step 3	**snmp-server group** *groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]	Configure a new SNMP group on the remote device. • For *groupname,* specify the name of the group. • Specify a security model: – **v1** is the least secure of the possible security models. – **v2c** is the second least secure model. It allows transmission of informs and integers twice the normal width. – **v3,** the most secure, requires you to select an authentication level: **auth**—Enables the Message Digest 5 (MD5) and the Secure Hash Algorithm (SHA) packet authentication. **noauth**—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.

	Command	Purpose
Step 4	**snmp-server user** *username groupname* {**remote** *host* [**udp-port** *port*]} {**v1** [**access** *access-list*] | **v2c** [**access** *access-list*] | **v3** [**encrypted**] [**access** *access-list*] [**auth** {**md5** | **sha**} *auth-password*]} [*priv* {**des** | **3des** | **aes** {**128** | **192** | **256**}} *priv-password*]	Add a new user for an SNMP group. • The *username* is the name of the user on the host that connects to the agent. • The *groupname* is the name of the group to which the user is associated. • Enter **remote** to specify a remote SNMP entity to which the user belongs and the hostname or IP address of that entity with the optional UDP port number. The default is 162. • Enter the SNMP version number (**v1**, **v2c**, or **v3**). If you enter **v3**, you have these additional options: – **encrypted** specifies that the password appears in encrypted format. This keyword is available only when the **v3** keyword is specified. – **auth** is an authentication level setting session that can be either the HMAC-MD5-96 (**md5**) or the HMAC-SHA-96 (**sha**) authentication level and requires a password string *auth-password* (not to exceed 64 characters). • If you enter **v3** and the switch is running the cryptographic software image, you can also configure a private (**priv**) encryption algorithm and password string *priv-password* (not to exceed 64 characters). – **priv** specifies the User-based Security Model (USM). – **des** specifies the use of the 56-bit DES algorithm. – **3des** specifies the use of the 168-bit DES algorithm. – **aes** specifies the use of the DES algorithm. You must select either 128-bit, 192-bit, or 256-bit encryption. • (Optional) Enter **access** *access-list* with a string (not to exceed 64 characters) that is the name of the access list.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**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	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

The following example shows how to configure a remote user to receive traps at the noAuthNoPriv security level when the SNMPv3 security model is enabled:

```
snmp-server group group1 v3 noauth
snmp-server user remoteuser1 group1 remote 10.12.8.4
snmp-server host 10.12.8.4 informs version 3 noauth remoteuser config
```

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.

Note Many commands use the word *traps* in the command syntax. Unless there is an option in the command to select either traps or informs, the keyword ***traps*** refers to traps, informs, or both. Use the **snmp-server host** global configuration command to specify whether to send SNMP notifications as traps or informs.

Table 14-4 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 14-4 Switch Notification Types

Notification Type Keyword	Description
bgp	Generates Border Gateway Protocol (BGP) state change traps. This option is only available when the IP services image is installed.
bridge	Generates STP bridge MIB traps.
bulkstat collection transfer	Generates a trap when an unsuccessful data collection or data transfer occurs or when the bulkstats file reaches the maximum size.
config	Generates a trap for SNMP configuration changes.
copy-config	Generates a trap for SNMP copy configuration changes.
cpu threshold	Generates a trap for CPU threshold violations.
entity	Generates a trap for SNMP entity changes.
envmon	Generates environmental monitor traps. You can enable any or all of these environmental traps: shutdown, status, supply, temperature.
ethernet	Generates an SNMP Ethernet trap.
flash	Generates SNMP FLASH notifications.
hsrp	Generates a trap for Hot Standby Router Protocol (HSRP) changes.
ipmulticast	Generates a trap for IP multicast routing changes.
mac-notification	Generates a trap for MAC address notifications.
msdp	Generates a trap for Multicast Source Discovery Protocol (MSDP) changes.
ospf	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.
pim	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.

Table 14-4 Switch Notification Types (continued)

Notification Type Keyword	Description
port-security	Generates SNMP port security traps. You can also set a maximum trap rate per second. The range is from 0 to 1000; the default is 0, which means that there is no rate limit. **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*
rtr	Generates a trap for the SNMP Response Time Reporter (RTR).
snmp	Generates a trap for SNMP-type notifications for authentication, cold start, warm start, link up or link down.
storm-control	Generates a trap for SNMP storm-control. You can also set a maximum trap rate per minute. The range is from 0 to 1000; the default is 0 (no limit is imposed; a trap is sent at every occurrence).
stpx	Generates SNMP STP Extended MIB traps.
syslog	Generates SNMP syslog traps.
tty	Generates a trap for TCP connections. This trap is enabled by default.
vlan-membership	Generates a trap for SNMP VLAN membership changes.
vlancreate	Generates SNMP VLAN created traps.
vlandelete	Generates SNMP VLAN deleted traps.

Note Though visible in the command-line help strings, the **flash insertion, flash removal, 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 14-4. 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.

BEFORE YOU BEGIN

Review the "Information About SNMP" section on page 14-1 and "Guidelines and Limitations" section on page 14-7.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**snmp-server engineID remote** *ip-address engineid-string*	Specify the engine ID for the remote host.
Step 3	**snmp-server user** *username groupname* {**remote** *host* [**udp-port** *port*]} {**v1** [**access** *access-list*] | **v2c** [**access** *access-list*] | **v3** [**encrypted**] [**access** *access-list*] [**auth** {**md5** | **sha**} *auth-password*]}	Configure an SNMP user to be associated with the remote host created in Step 2. **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.
Step 4	**snmp-server group** *groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]	Configure an SNMP group.
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. **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. • (Optional) For *notification-type*, use the keywords listed in Table 14-4 on page 14-14. If no type is specified, all notifications are sent.

	Command	Purpose
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 14-4 on page 14-14, 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.

To remove the specified host from receiving traps, use the **no snmp-server host** *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.

EXAMPLE

The following example specifies the engine ID for the remote host, an SNMP user to be associated with the remote host, an SNMP group, the host that will receive the informs:

```
Switch(config)# snmp-server engineID remote 172.16.20.3 80000009030000B064EFE100
Switch(config)# snmp-server user abcd public remote 172.16.20.3 v3 encrypted auth md5
publichost remotehostusers
Switch(config)# snmp-server group GROUP1 v2c auth read viewA write viewA notify viewB
Switch(config)# snmp-server host example.com informs version 3 public
Switch(config)# snmp-server enable traps bgp
Switch(config)# exit
```

Setting the Agent Contact and Location Information

Set the system contact and location of the SNMP agent so that these descriptions can be accessed through the configuration file.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**snmp-server contact** *text*	Set the system contact string.
Step 3	**snmp-server location** *text*	Set the system location string.
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.

EXAMPLE

```
Switch(config)# snmp-server contact Admin at 21555
Switch(config)# snmp-server location Building 3/Room 222
```

Limiting TFTP Servers Used Through SNMP

Follow this procedure to limit the TFTP servers used for saving and loading configuration files through SNMP to the servers specified in an access list.

BEFORE YOU BEGIN

Obtain the IP address of the TFTP servers that can access the switch.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**snmp-server tftp-server-list** *access-list-number*	Limit TFTP servers used for configuration file copies through SNMP to the servers in the access list. • For *access-list-number*, enter an IP standard access list numbered from 1 to 99 and 1300 to 1999.

	Command	Purpose
Step 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	Create a standard access list, repeating the command as many times as necessary. • For *access-list-number*, enter the access list number specified in Step 2. • The **deny** keyword denies access if the conditions are matched. The **permit** keyword permits access if the conditions are matched. • For *source*, enter the IP address of the TFTP servers that can access the switch. • (Optional) For *source-wildcard*, enter the wildcard bits, in dotted decimal notation, to be applied to the source. Place ones in the bit positions that you want to ignore. Recall that the access list is always terminated by an implicit deny statement for everything.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

The following example shows how to limit the TFTP servers that can be used for copying configuration files through SNMP to the servers in access list 44:

```
Switch(config)# snmp-server tftp-server-list 44
```

Configuring MIB Data Collection and Transfer

This section includes basic configuration for MIB data collection. For more information, see the chapter "Periodic MIB Data Collection and Transfer Mechanism" in the *SNMP Configuration Guide, Cisco IOS Release 15M&T*.

Configuring a Bulk-Statistics Object List and Schema Options

BEFORE YOU BEGIN

- Review the "MIB Data Collection and Transfer" section on page 14-6.
- Know what MIB information you want to monitor on your network devices, and the OIDs or object names for the MIB objects to be monitored.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**snmp mib bulkstat object-list** *list-name*	Define an SNMP bulk-statistics object list, and enter bulk-statistics object-list configuration mode.
Step 3	**add** {*object-name* | *oid*}	Add a MIB object to the bulk-statistics object list. • For *object-name,* 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. • For *oid,* enter the Object ID of the MIB object to add to the list. 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.
Step 4	**exit**	Return to global configuration mode.
Step 5	**snmp mib bulkstat schema** *schema-name*	Name the SNMP bulk statistics schema, and enter bulk-statistics schema configuration mode.
Step 6	**object-list** *list-name*	Specify the bulk-statistics object list to be included in this schema. Specify only one object list per schema. If multiple **object-list** commands are entered, the most recent command overwrites the previous command.
Step 7	**instance** {**exact** | **wild**} {**interface** *interface-id* | **oid** *oid*}	Specify the instance information for objects in this schema. Enter only one **instance** command per schema. If multiple **instance** commands are entered, the most recent command overwrites the previous command. • Enter **exact** when the specified instance appended to the object list is the complete OID. • Enter **wild** when all subindices of the specified OID belong to the schema. • Enter an **interface** *interface-id* to specify an interface ID instead of an instance OID. • Enter **oid** *oid* to specify an instance OID for the schema.
Step 8	**poll interval** *interval*	Set the time interval in minutes for collection of data from the object instances specified in the schema. The range is from 1 to 20000 minutes; the default is 5 minutes.
Step 9	**end**	Return to privileged EXEC mode.
Step 10	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

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
```

Configuring Bulk-Statistics Transfer Options

BEFORE YOU BEGIN

Create a bulk-statistics schema as described in the "Configuring a Bulk-Statistics Object List and Schema Options" procedure on page 14-19.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**snmp mib bulkstat transfer** *transfer-id*	Identify the transfer configuration with a name, and enter bulk-statistics transfer configuration mode.
Step 3	**buffer-size** *bytes*	(Optional) Specify the maximum size for the bulk-statistics data file in bytes. The range is from 1024 to 2147483647 bytes; the default is 2048 bytes.
Step 4	**format** {**bulkBinary** | **bulkASCII** | **schemaASCII**}	(Optional) Specify the format of the bulk-statistics data file. The default is **schemaASCII**.
Step 5	**schema** *schema-name*	Specify the bulk-statistics schema to be transferred. Repeat this command for as many schemas as desired. You can associate multiple schemas with a transfer configuration.
Step 6	**transfer-interval** *minutes*	(Optional) Specify the length of time that the system should collect MIB data before attempting the transfer operation. The valid range is from 1 to 2147483647 minutes; the default is 30 minutes. The transfer interval is the same as the collection interval.
Step 7	**url primary** *URL*	Specify the NMS (host) that the bulk-statistics file should be transferred to and the protocol to use for transfer (FTP, RCP, or TFTP). You also can optionally enter the **url secondary** command to specify a backup transfer destination.
Step 8	**retry** *number*	(Optional) Specify the number of transmission retries. The range is from 1 to 100; the default is 0 (no retries).
Step 9	**retain** *minutes*	(Optional) Specify how long the bulk-statistics file should be kept in system memory. The valid range is 0 to 20000 minutes; the default is 0 (the file is deleted immediately after a successful transfer).

	Command	Purpose
Step 10	**enable**	Begin the bulk-statistics data collection and transfer process for this configuration. You must enter this command to start periodic collection and transfer.
Step 11	**end**	Return to privileged EXEC mode.
Step 12	**show mib bulk transfer**	Verify your entries.
Step 13	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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.

EXAMPLE

This is an example of configuring the bulk-statistics transfer and enabling the collection process:

```
Switch(config)# snmp mib bulkstat transfer testtransfer
Switch(config-bulk-tr)# format schemaASCII
Switch(config-bulk-tr)# buffer-size 2147483647
Switch(config-bulk-tr)# schema 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 CPU Threshold Notification

CPU threshold notification can serve as a way to notify network operations staff when a predefined threshold of CPU usage is surpassed. When this occurs an SNMP trap message for the top users of the CPU is sent to the configured NMS systems.

BEFORE YOU BEGIN

Be familiar with the CPU utilization on your switch.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**process cpu statistics limit entry-percentage** *number* [**size** *seconds*]	Set the process entry limit and the size of the history table for CPU utilization statistics. • For **entry-percentage** *number,* enter the percentage (1 to 100) of CPU utilization that a process must use to become part of the history table. • (Optional) For **size** *seconds*, set the duration of time in seconds for which CPU statistics are stored in the history table. The range is from 5 to 86400 seconds; the default is 600.
Step 3	**process cpu threshold type** {**total** | **process** | **interrupt**} **rising** *percentage* **interval** *seconds* [**falling** *percentage* **interval** *seconds*]	Set CPU threshold notification types and values. • Set the **threshold type** to **total** CPU utilization, CPU **process** utilization, or CPU **interrupt** utilization. • For **rising** *percentage,* enter the percentage (1 to 100) of CPU resources that triggers a CPU threshold notification when exceeded. • For **interval** *seconds,* enter the duration of the CPU threshold violation in seconds (5 to 86400) that must be met to trigger a CPU threshold notification. The default is 5 seconds. • (Optional) Set a **falling** *percentage* **interval** *seconds* that, when usage falls below this level for the configured interval, triggers a CPU threshold notification. The percentage must be equal to or less than the rising percentage. The default is for the falling percentage to be the same value as the rising percentage.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

The following example shows how to set an entry limit at 40 percent and a size of 300 seconds:

```
Switch(config)# process cpu statistics limit entry-percentage 40 size 300
```

This example configures the system to send a notification when the CPU utilization exceeds 50% for a period of 60 seconds. Because a falling percentage threshold is not specified, the system uses the same parameters as the configured rising threshold. This means that a notification will also be sent out when the CPU utilization falls under 50% utilization for a period of 60 seconds.

```
Switch(config)# snmp-server enable traps cpu threshold < - - Enables the cpu threshold
trap to be sent

Switch(config)# process cpu threshold type total rising 50 interval 60
```

Verifying Configuration

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 listed below to display SNMP information. For information about the fields in the displays, see the *Cisco IOS Configuration Fundamentals Command Reference, Release 15.2M&T*.

Command	Purpose
show snmp	Displays SNMP statistics.
show snmp engineID [**local** | **remote**]	Displays information on the local SNMP engine and all remote engines that have been configured on the device.
show snmp group	Displays information on each SNMP group on the network.
show snmp mib bulk transfer	Displays transfer status of files generated by the Periodic MIB Data Collection and Transfer Mechanism (bulk statistics feature).
show snmp pending	Displays information on pending SNMP requests.
show snmp sessions	Displays information on the current SNMP sessions.
show snmp user	Displays information on each SNMP user name in the SNMP users 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.

Configuration Example

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
```

Related Documents

- Cisco IOS SNMP Support Command Reference
- Cisco IOS Master Command List, All Releases
- Cisco IOS Configuration Fundamentals Command Reference, Release 15.2M&T
- SNMP Configuration Guide, Cisco IOS Release 15M&T

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

Configuring Embedded Event Manager

Embedded Event Manager (EEM) is a distributed and customized approach to event detection and recovery within a Cisco IOS device. EEM offers the ability to monitor events and take informational, corrective, or any other EEM action when the monitored events occur or when a threshold is reached. An EEM policy defines an event and the actions to be taken when that event occurs.

This chapter describes how to configure EEM and how to use it to monitor and manage the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*.

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 15-9.

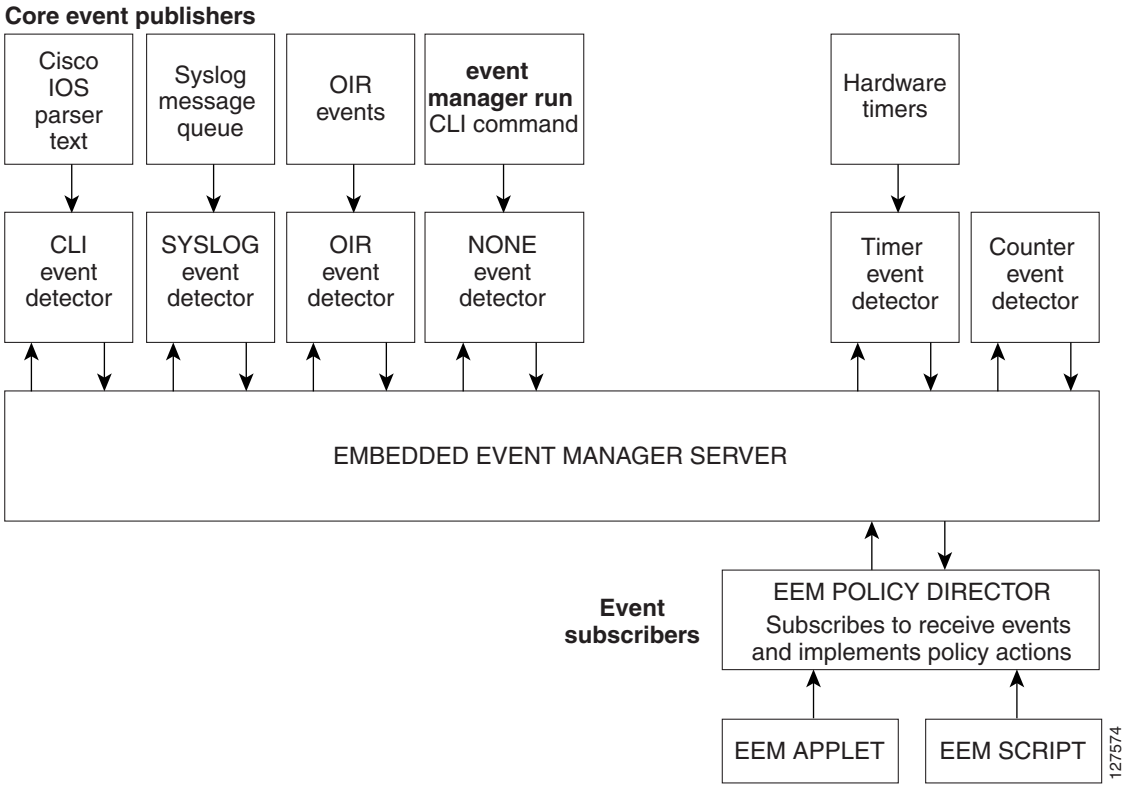
This chapter includes these sections:

Information About Embedded Event Manager

EEM monitors key system events and then acts on them through a set policy. This policy is a programmed script that you can use to customize a script to invoke an action based on a given set of events occurring. The script generates actions such as generating custom syslog or Simple Network Management Protocol (SNMP) traps, invoking CLI commands, forcing a failover, and so forth. The event management capabilities of EEM are useful because not all event management can be managed from the switch and because some problems compromise communication between the switch and the external network management device. Network availability is improved if automatic recovery actions are performed without rebooting the switch.

Figure 15-1 shows the relationship between the EEM server, the core event publishers (event detectors), and the event subscribers (policies). The event publishers screen events and when there is a match on an event specification that is provided by the event subscriber. Event detectors notify the EEM server when an event occurs. The EEM policies then implement recovery based on the current state of the system and the actions specified in the policy for the given event.

Figure 15-1 Embedded Event Manager Core Event Detectors



See the *EEM Configuration for Cisco Integrated Services Router Platforms Guide* for examples of EEM deployment.

This section includes the following topics:

Event Detectors

EEM software programs known as event detectors determine when an EEM event occurs. Event detectors are separate systems that provide an interface between the agent being monitored, for example SNMP, and the EEM polices where an action can be implemented.

EEM allows these event detectors:

- Application-specific event detector—Allows any EEM policy to publish an event.
- IOS CLI event detector—Generates policies based on the commands entered through the CLI.
- Generic Online Diagnostics (GOLD) event detector—Publishes an event when a GOLD failure event is detected on a specified card and subcard.
- Counter event detector—Publishes an event when a named counter crosses a specified threshold.
- Interface counter event detector—Publishes an event when a generic Cisco IOS interface counter for a specified interface crosses a defined threshold. A threshold can be specified as an absolute value or an incremental value. For example, if the incremental value is set to 50, an event would be published when the interface counter increases by 50.

  This detector also publishes an event about an interface based on the rate of change for the entry and exit values.
- None event detector—Publishes an event when the **event manager run** CLI command executes an EEM policy. EEM schedules and runs policies on the basis on an event specification within the policy itself. An EEM policy must be manually identified and registered before the **event manager run** command executes.
- Online insertion and removal event detector—Publishes an event when a hardware insertion or removal (OIR) event occurs.
- Remote procedure call (RPC) event detector—Invokes EEM policies from outside the switch over an encrypted connecting using Secure Shell (SSH) and uses Simple Object Access Protocol (SOAP) data encoding for exchanging XML-based messages. It also runs EEM policies and then gets the output in a SOAP XML-formatted reply.
- SNMP event detector—Allows a standard SNMP MIB object to be monitored and an event to be generated when
  - The object matches specified values or crosses specified thresholds.
  - The SNMP delta value, the difference between the monitored Object Identifier (OID) value at the beginning the period and the actual OID value when the event is published, matches a specified value.
- SNMP notification event detector—Intercepts SNMP trap and inform messages received by the switch. The event is generated when an incoming message matches a specified value or crosses a defined threshold.
- Syslog event detector—Allows for screening syslog messages for a regular expression pattern match. The selected messages can be further qualified, requiring that a specific number of occurrences be logged within a specified time. A match on a specified event criteria triggers a configured policy action.
- Timer event detector—Publishes events for the following different types of timers:
  - An absolute-time-of-day timer publishes an event when a specified absolute date and time occurs.
  - A countdown timer publishes an event when a timer counts down to zero.
  - A watchdog timer publishes an event when a timer counts down to zero. The timer automatically resets itself to its initial value and starts to count down again.
  - A CRON timer publishes an event by using a UNIX standard CRON specification to define when the event is to be published. A CRON timer never publishes events more than once per minute.

- Watchdog event detector (IOSWDSysMon)— Publishes an event when one of these events occurs:
  - CPU utilization for a Cisco IOS process crosses a threshold.
  - Memory utilization for a Cisco IOS process crosses a threshold.

  Two events can be monitored at the same time, and the event publishing criteria requires that one or both events cross their specified thresholds.

Embedded Event Manager Actions

These actions occur in response to an event:

- Modifying a named counter.
- Publishing an application-specific event.
- Generating an SNMP trap.
- Generating prioritized syslog messages.
- Reloading the Cisco IOS software.

Embedded Event Manager Policies

EEM can monitor events and provide information, or take corrective action when the monitored events occur or a threshold is reached. An EEM policy is an entity that defines an event and the actions to be taken when that event occurs.

There are two types of EEM policies: an applet or a script. An applet is a simple policy that is defined within the CLI configuration. It is a concise method for defining event screening criteria and the actions to be taken when that event occurs. Scripts are defined on the networking device by using an ASCII editor. The script, which can be a bytecode (.tbc) and text (.tcl) script, is then copied to the networking device and registered with EEM. You can also register multiple events in a .tcl file.

Cisco enhancements to TCL in the form of keyword extensions facilitate the development of EEM policies. These keywords identify the detected event, the subsequent action, utility information, counter values, and system information.

For complete information on configuring EEM policies and scripts, see the *Embedded Event Manager Configuration Guide, Cisco IOS Release 15M&T*.

Embedded Event Manager Environment Variables

EEM uses environment variables in EEM policies. These variables are defined in an EEM policy tool command language (TCL) script by running a CLI command and the **event manager environment** command.

User-defined variables

Defined by the user for a user-defined policy.

- Cisco-defined variables

  Defined by Cisco for a specific sample policy.

- Cisco built-in variables (available in EEM applets)

  Defined by Cisco and can be read-only or read-write. The read-only variables are set by the system before an applet starts to execute. The single read-write variable, _exit_status, allows you to set the exit status for policies triggered from synchronous events.

Cisco-defined environment variables and Cisco system-defined environment variables might apply to one specific event detector or to all event detectors. Environment variables that are user-defined or defined by Cisco in a sample policy are set by using the **event manager environment** global configuration command. You must defined the variables in the EEM policy before you register the policy.

For information about the environmental variables that EEM supports, see the *Embedded Event Manager Configuration Guide, Cisco IOS Release 15M&T*.

EEM 3.2

EEM 3.2 introduces these event detectors:

- Neighbor Discovery—Provides the ability to publish a policy to respond to automatic neighbor detection when:
  - a Cisco Discovery Protocol (CDP) cache entry is added, deleted, or updated.
  - a Link Layer Discovery Protocol (LLDP) cache entry is added, deleted or updated.
  - an interface link status changes.
  - an interface line status changes.
- Identity—Generates an event when AAA authorization and authentication is successful, when failure occurs, or after normal user traffic on the port is allowed to flow.
- Mac-Address-Table—Generates an event when a MAC address is learned in the MAC address table.

Note The Mac-Address-Table event detector is supported only on switch platforms and can be used only on Layer 2 interfaces where MAC addresses are learned. Layer 3 interfaces do not learn addresses, and routers do not usually support the MAC address-table infrastructure needed to notify EEM of a learned MAC address.

EEM 3.2 also introduces CLI commands to support the applets to work with the new event detectors.

Prerequisites

- Review the "Information About Embedded Event Manager" section on page 15-1.
- If the **action snmp-trap** command is used, the **snmp-server enable traps event-manager** command must be enabled to permit SNMP traps to be sent from the Cisco IOS device to the SNMP server. Other relevant **snmp-server** commands must also be configured; for details see the **action snmp-trap** command page.

Guidelines and Limitations

For complete information about configuring embedded event manager, see the *Embedded Event Manager Configuration Guide, Cisco IOS Release 15M&T*.

Default Settings

No EEM policies are registered.

Configuring Embedded Event Manager

Registering and Defining an Embedded Event Manager Applet

BEFORE YOU BEGIN

Review the "Information About Embedded Event Manager" section on page 15-1.

DETAILED STEPS

Note Only one event applet command is allowed in an EEM applet. Multiple action applet commands are permitted. If you do not specify the **no event** and **no action** commands, the applet is removed when you exit configuration mode.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**event manager applet** *applet-name*	Register the applet with EEM and enter applet configuration mode.
Step 3	**event snmp oid** *oid-value* **get-type** {**exact** | **next**} **entry-op** {**gt** | **ge** | **eq** | **ne** | **lt** | **le**} **entry-val** *entry-val* [**exit-comb** {**or** |**and**}] [**exit-op** {**gt** | **ge** | **eq** | **ne** | **lt** | **le**}] [**exit-val** **exit-val**] [**exit-time** *exit-time-val*] **poll-interval** *poll-int-val*	Specify the event criteria that causes the EEM applet to run. (Optional) Exit criteria. If exit criteria are not specified, event monitoring is re-enabled immediately.

	Command	Purpose
Step 4	**action label syslog** [**priority** *priority-level*] **msg** *msg-text*	Specify the action when an EEM applet is triggered. Repeat this action to add other CLI commands to the applet. • (Optional) The priority keyword specifies the priority level of the syslog messages. If selected, you need to define the priority-level argument. • For *msg-text*, the argument can be character text, an environment variable, or a combination of the two.
Step 5	**end**	Exit applet configuration mode and return to privileged EXEC mode.

EXAMPLE

The following example shows how to configure an EEM applet that runs when there is an exact match on the value of a specified SNMP object ID that represents the amount of current process memory.

```
Switch(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.48.1.1.1.6.1 get-type exact entry-op
lt entry-val 5120000 poll-interval 10
```

These examples show actions that are taken in response to an EEM event:

```
Switch(config-applet)# action 1.0 syslog priority critical msg "Memory exhausted; current
available memory is $_snmp_oid_val bytes"

Switch (config-applet)# action 2.0 force-switchover
```

Registering and Defining an Embedded Event Manager TCL Script

BEFORE YOU BEGIN

Review the "Information About Embedded Event Manager" section on page 15-1.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 1	**show event manager environment** [**all** | *variable-name*]	(Optional) The **show event manager environment** command displays the name and value of the EEM environment variables. • (Optional) The **all** keyword displays the EEM environment variables. • (Optional) The *variable-name* argument displays information about the specified environment variable.
Step 2	**configure terminal**	Enter global configuration mode.
Step 3	**event manager environment** *variable-name string*	Configure the value of the specified EEM environment variable. Repeat this step for all the required environment variables.

	Command	Purpose
Step 4	**event manager policy** *policy-file-name* [**type system**] [**trap**]	Register the EEM policy to run when the specified event defined within the policy occurs.
Step 5	**exit**	Exit global configuration mode and return to privileged EXEC mode.

EXAMPLE

This example shows the sample output for the show event manager environment command:

```
Switch# show event manager environment all
No.  Name                          Value
1    _cron_entry                   0-59/2 0-23/1 * * 0-6
2    _show_cmd                     show ver
3    _syslog_pattern               .*UPDOWN.*Ethernet1/0.*
4    _config_cmd1                  interface Ethernet1/0
5    _config_cmd2                  no shut
```

This example shows a CRON timer environment variable, which is assigned by the software, to be set to every second minute, every hour of every day:

```
Switch (config)# event manager environment_cron_entry 0-59/2 0-23/1 * * 0-6
```

This example shows the sample EEM policy named *tm_cli_cmd.tcl* registered as a system policy. The system policies are part of the Cisco IOS image. User-defined TCL scripts must first be copied to flash memory.

```
Switch (config)# event manager policy tm_cli_cmd.tcl type system
```

Verifying Configuration

To display information about EEM, including EEM registered policies and EEM history data, see the *Cisco IOS Embedded Event Manager Command Reference*.

Configuration Example

This example shows the output for EEM when one of the fields specified by an SNMP object ID crosses a defined threshold:

```
Switch(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.48.1.1.1.6.1 get-type exact entry-op
lt entry-val 5120000 poll-interval 10
```

These examples show actions that are taken in response to an EEM event:

```
Switch(config-applet)# action 1.0 syslog priority critical msg "Memory exhausted; current
available memory is $_snmp_oid_val bytes"

Switch (config-applet)# action 2.0 force-switchover
```

This example shows the sample output for the show event manager environment command:

```
Switch# show event manager environment all
No.  Name                          Value
1    _cron_entry                   0-59/2 0-23/1 * * 0-6
2    _show_cmd                     show ver
```

```
3    _syslog_pattern              .*UPDOWN.*Ethernet1/0.*
4    _config_cmd1                 interface Ethernet1/0
5    _config_cmd2                 no shut
```

This example shows a CRON timer environment variable, which is assigned by the software, to be set to every second minute, every hour of every day:

```
Switch (config)# event manager environment_cron_entry 0-59/2 0-23/1 * * 0-6
```

This example shows the sample EEM policy named *tm_cli_cmd.tcl* registered as a system policy. The system policies are part of the Cisco IOS image. User-defined TCL scripts must first be copied to flash memory.

```
Switch (config)# event manager policy tm_cli_cmd.tcl type system
```

Related Documents

- Cisco IOS Master Command List, All Releases
- Cisco IOS Embedded Event Manager Command Reference
- Cisco IOS 15.2M&T Command References, Network Management
- Embedded Event Manager Configuration Guide, Cisco IOS Release 15M&T

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

Configuring Cisco IOS IP SLAs Operations

This chapter describes how to use Cisco IOS IP Service Level Agreements (SLAs) and the IETF Two-Way Active Measurement Protocol (TWAMP) on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *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 documents listed in the "Related Documents" section on page 16-6.

This chapter includes the following sections:

Information About 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).

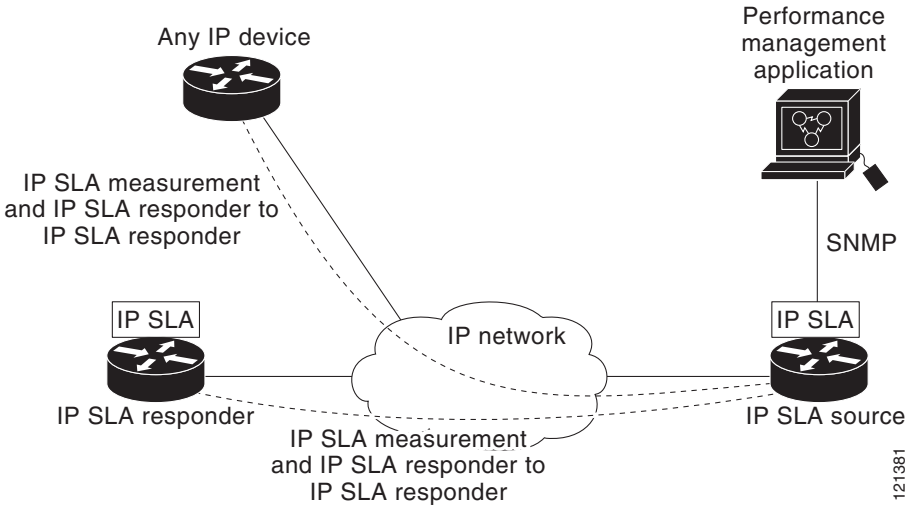
This section includes the following topics:

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 16-1 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 16-1 Cisco IOS IP SLAs Operation



To implement IP SLAs network performance measurement, 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.

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.

Figure 16-1 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.

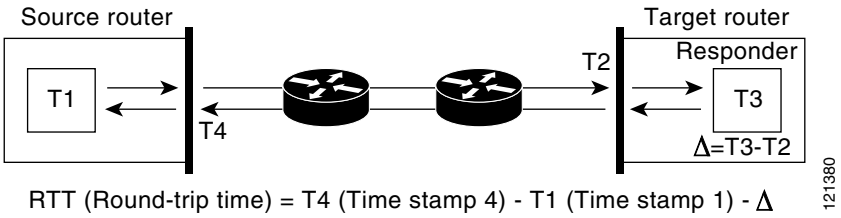
Response Time Computation for IP SLAs

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 16-2 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.

Figure 16-2 Cisco IOS IP SLAs Responder Time Stamping



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.

Prerequisites

Your IP network is operational and you can access the destination device.

Guidelines and Limitations

This chapter does not include configuration information for all available operations. For details about configuring other operations, see the *IP SLAs Configuration Guide, Cisco IOS Release 15M&T*.

Default Settings

No IP SLAs operations are configured.

Configuring IP SLAs Operations

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. The responder must be enabled before you configure IP SLAs operations that require a responder. Follow these steps to configure the IP SLAs responder on the target device (the operational target).

BEFORE YOU BEGIN

Review the "Information About Cisco IOS IP SLAs" section on page 16-1.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip sla responder** {**tcp-connect** | **udp-echo**} **ipaddress** *ip-address* **port** *port-number*	Configure the switch as an IP SLAs responder. The keywords have these meanings: • **tcp-connect**—Enable the responder for TCP connect operations. • **udp-echo**—Enable the responder for User Datagram Protocol (UDP) echo or jitter operations. • **ipaddress** *ip-address*—Enter the destination IP address. • **port** *port-number*—Enter the destination port number. **Note** The IP address and port number must match those configured on the source device for the IP SLAs operation.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show ip sla responder**	Verify the IP SLAs responder configuration on the device.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable the IP SLAs responder, enter the **no ip sla responder** global configuration command.

EXAMPLE

This example shows how to configure the device as a responder for the UDP jitter IP SLAs operation:

```
Switch(config)# ip sla responder udp-echo 172.29.139.134 5000
```

Verifying Configuration

Command	Purpose
show ip sla authentication	Display IP SLAs authentication information.
show ip sla responder	Display information about the IP SLAs responder.

Related Documents

- IP SLAs Configuration Guide, Cisco IOS Release 15M&T
- Cisco IOS IP SLAs Command Reference

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

Configuring Ethernet OAM, CFM, and E-LMI

This chapter describes Ethernet Operations, Administration, and Maintenance (OAM) on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*.

Ethernet OAM is a protocol for installing, monitoring, and troubleshooting Ethernet networks to increase management capability within the context of the overall Ethernet infrastructure. The switch supports IEEE 802.1ag Connectivity Fault Management (CFM), Ethernet Local Management Interface (E-LMI), and IEEE 802.3ah Ethernet OAM discovery, link monitoring, remote fault detection, and remote loopback. It also supports IP Service Level Agreements (SLAs) for CFM, and ITU-T Y.1731 fault management. Ethernet OAM manager controls the interworking between any two of the protocols (CFM, E-LMI, and OAM).

This chapter provides information about configuring CFM, E-LMI, and the Ethernet OAM protocol. It defines the differences between the ratified CFM 802.1ag standard (draft 8.1) and the previous version supported on the switch in Cisco IOS (draft 1.0). It also includes configuration information for CFM ITU-TY.1731 fault management support in this release.

For complete command and configuration information for Ethernet OAM,CFM, E-LMI, and Y.1731, see the documents listed in the "Related Documents" section on page 17-63.

Note The Service Diagnostics 2.0 C FM diagnostic script is part of the 12.2(53)EX release:
http://www.cisco.com/en/US/prod/iosswrel/ps6537/ps6555/ps9424/cisco_ios_service_diagnostics_scripts.html
Refer to the Service Diagnostic 2.0 user guide:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps9424/whitepaper_c11-566741.html

This chapter contains the following sections:

Information About Ethernet CFM

Ethernet CFM is an end-to-end per-service-instance (per VLAN) Ethernet layer OAM protocol that includes proactive connectivity monitoring, fault verification, and fault isolation. End-to-end can be provider-edge-to-provider-edge (PE-to-PE) device or customer-edge-to-customer-edge (CE-to-CE) device. Ethernet CFM, as specified by 802.1ag, is the standard for Layer 2 ping, Layer 2 traceroute, and end-to-end connectivity check of the Ethernet network.

These sections contain conceptual information about Ethernet CFM:

CFM Domain

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 17-1, 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 17-2, 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 administrating organizations. CFM exchanges messages and performs operations on a per-domain basis.

Figure 17-1 CFM Maintenance Domains

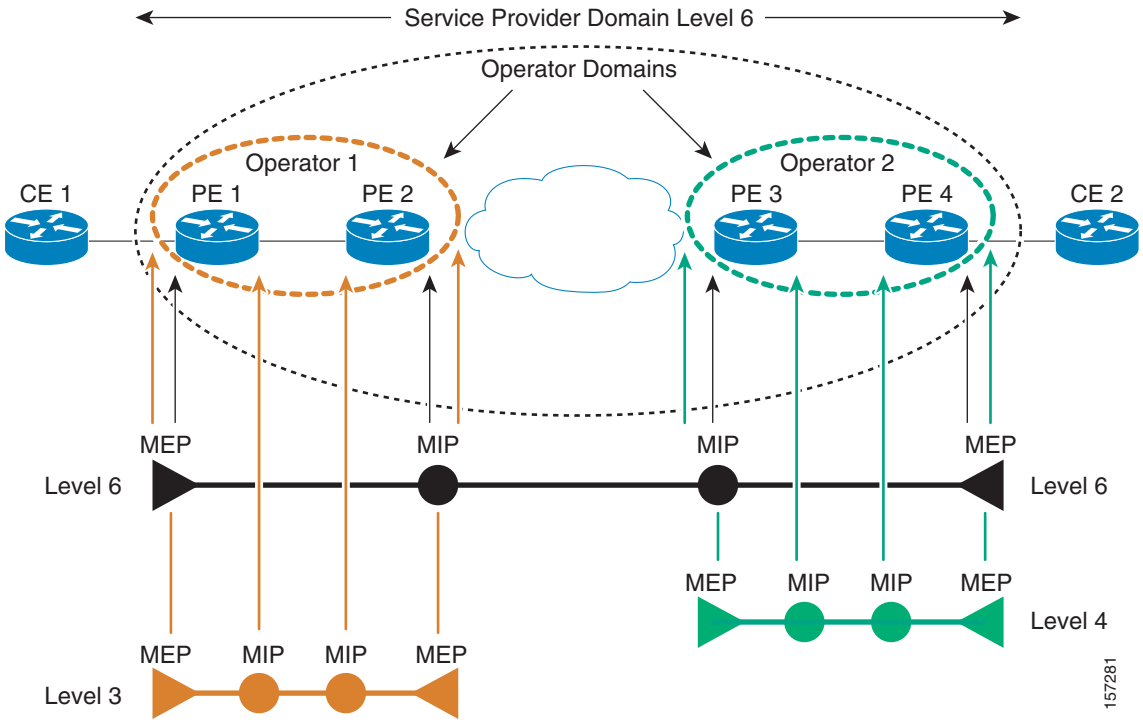
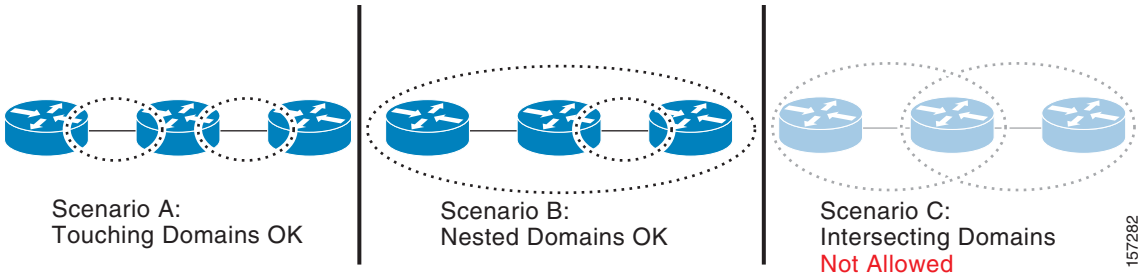


Figure 17-2 Allowed Domain Relationships



Maintenance Associations and Maintenance Points

A maintenance association (MA) identifies a service that can be uniquely identified within the maintenance domain. The CFM protocol runs within a maintenance association. A maintenance point is a demarcation point on an interface that participates in CFM within a maintenance domain. Maintenance points drop all lower-level frames and forward all higher-level frames. There are two types of maintenance points:

- Maintenance end points (MEPs) are points at the edge of the domain that define the boundaries and confine CFM messages within these boundaries. *Outward facing* or *Down* MEPs communicate through the wire side (connected to the port). *Inward facing* or *Up* MEPs communicate through the relay function side, not the wire side.

Note CFM draft 1 referred to inward and outward-facing MEPs. CFM draft 8.1 refers to up and down MEPs, respectively. This document uses the CFM 8.1 terminology for direction.

CFM draft 1 supported only up MEPs on a per-port or per-VLAN basis. CFM 802.1ag supports up and down per-VLAN MEPs, as well as port MEPs, which are untagged down MEPs that are not associated with a VLAN. Port MEPs are configured to protect a single hop and used to monitor link state through CFM. If a port MEP is not receiving continuity check messages from its peer (static remote MEP), for a specified interval, the port is put into an operational down state in which only CFM and OAM packets pass through, and all other data and control packets are dropped.

- An up MEP sends and receives CFM frames through the relay function. It drops all CFM frames at its level or lower that come from the wire side, except traffic going to the down MEP. For CFM frames from the relay side, it processes the frames at its level and drops frames at a lower level. The MEP transparently forwards all CFM frames at a higher level, regardless of whether they are received from the relay or wire side. If the port on which MEP is configured is blocked by STP, the MEP can still send or receive CFM messages through the relay function. CFM runs at the provider maintenance level (UPE-to-UPE), specifically with up MEPs at the user network interface (UNI).

Note A UNI in the context of CFM and OAM manager is not the same as a UNI port type. The CFM UNI can be a UNI, an enhanced network interface (ENI), or a network node interface (NNI) port type. The switch rate-limits all incoming CFM messages at a fixed rate of 500 frames per second. In CFM draft 1, the control-plane security rate-limited incoming CFM messages only on UNI and ENI port types.

- A down MEP sends and receives CFM frames through the wire connected to the port on which the MEP is configured. It drops all CFM frames at its level or lower that come from the relay side. For CFM frames from the wire side, it processes all CFM frames at its level and drops CFM frames at lower levels except traffic going to the other lower-level down MEP. The MEP transparently forwards all CFM frames at a higher level, regardless of whether they are received from the relay or through the wire.

- Maintenance intermediate points (MIPs) are internal to a domain, not at the boundary, and respond to CFM only when triggered by traceroute and loopback messages. They forward CFM frames received from MEPs and other MIPs, drop all CFM frames at a lower level (unless MIP filtering is enabled), and forward all CFM frames at a higher level and at a lower level and regardless of whether they are received from the relay or wire side. When MIP filtering is enabled, the MIP drops CFM frames at a lower level. MIPs also catalog and forward continuity check messages (CCMs), but do not respond to them.

  In the first draft of CFM, MIP filtering was always enabled. In draft 8.1, MIP filtering is disabled by default, and you can configure it to be enabled or disabled. When MIP filtering is disabled, all CFM frames are forwarded.

  You can manually configure a MIP or configure the switch to automatically create a MIP. You can configure a MEP without a MIP. In case of a configuration conflict, manually created MIPs take precedence over automatically created MIPs.

  If port on which the MEP is configured is blocked by Spanning-Tree Protocol (STP), the MIP can receive and might respond to CFM messages from both the wire and relay side, but cannot forward any CFM messages. This differs from CFM draft 1, where STP blocked ports could not send or receive CFM messages.

CFM Messages

CFM uses standard Ethernet frames distinguished by EtherType or (for multicast messages) by MAC address. All CFM messages are confined to a maintenance domain and to a service-provider VLAN (S-VLAN). These CFM messages are supported:

- Continuity Check (CC) messages—multicast heartbeat messages exchanged periodically between MEPs that allow MEPs to discover other MEPs within a domain and allow MIPs to discover MEPs. CC messages are configured to a domain or VLAN. Enter the **continuity-check** Ethernet service configuration command to enable CCM.

  The default continuity check message (CCM) interval on the switch is 10 seconds. You can set it to be 100 ms, 1 second, 1 minute, or 10 minutes by entering the **continuity-check interval** Ethernet service mode command. Because faster CCM rates are more CPU intensive, we do not recommend configuring a large number of MEPs running at 100 ms intervals.
- Loopback messages—unicast or multicast frames transmitted by a MEP at administrator request to verify connectivity to a particular maintenance point, indicating if a destination is reachable. A loopback message is similar to an Internet Control Message Protocol (ICMP) ping message. Refer to the **ping ethernet** privileged EXEC command.
- Traceroute messages—multicast frames transmitted by a MEP at administrator request to track the path (hop-by-hop) to a destination MEP. Traceroute messages are similar in concept to UDP traceroute messages. Refer to the **traceroute ethernet** privileged EXEC command.

Crosscheck Function and Static Remote MEPs

The crosscheck function is a timer-driven post-provisioning service verification between dynamically configured MEPs (using crosscheck messages) and expected MEPs (by configuration) for a service. It verifies that all endpoints of a multipoint service are operational. The crosscheck function is performed only 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. In CFM draft 1, fault alarms were sent instantaneously when detected. In CFM 802.1ag, you can configure the priority level of alarms that trigger an SNMP trap or syslog message. You can also configure a delay period before a fault alarm is sent and the time before the alarm is reset.

Configuration Error List

CFM configuration errors in CFM 802.1ag can be misconfigurations or extra configuration commands detected during MEP configuration. They can be caused by overlapping maintenance associations. For example, if you create a maintenance association with a VLAN list and a MEP on an interface, a potential

leak error could occur if other maintenance associations associated with the same VLAN exist at a higher level without any MEPs configured. You can display the configuration error list, which is informational only, by entering the **show ethernet cfm errors configuration** privileged EXEC command.

CFM Version Interoperability

When customers upgrade their network from the Cisco CFM draft 1 to IEEE standardized 802.1ag CFM, they might not upgrade all equipment at the same time, which could result in a mix of Cisco CFM draft 1 and IEEE standardized CFM devices in the network. CFM areas are regions in a network running Cisco CFM draft 1 software. Internal area bridges are all Cisco devices running CFM draft 1, and external area bridges are devices (Cisco or third-party devices) running IEEE standardized 802.1ag CFM.

Devices at the edge of these areas perform message translation. Translation is not needed for maintenance domains that do not span different areas (that is, where CFM messages end on a port on the device) since the port can respond in the same message format as was received. However, for maintenance domains that span across two areas, the device must translate the CFM message appropriately before sending it on to the other area.

When designing a network with CFM areas, follow these guidelines:

- Whenever possible, group devices with the same CFM version together.
- Minimize the number of boundaries between CFM clusters, minimizing the number of devices that must perform translation.
- Never mix CFM versions on a single segment.

When the network does use both versions of CFM, you can enable translation on the CFM 802.1ag port that is connected to the draft 1 device by entering the **ethernet cfm version cisco** interface configuration command.

Note If you are running CFM draft 1 and upgrade to a software version that supports CFM 802.1ag, the switch automatically transfers the draft 1 configuration to the standard.

IP SLAs Support for CFM

The switch supports CFM with IP Service Level Agreements (SLAs), which provides the ability to gather Ethernet layer network performance metrics. Available statistical measurements for the IP SLAs CFM operation include round-trip time, jitter (interpacket delay variance), and packet loss. You can schedule multiple IP SLAs operations and use Simple Network Management Protocol (SNMP) trap notifications and syslog messages for proactive threshold violation monitoring.

For more information about IP SLAs, see Chapter 16, “Configuring Cisco IOS IP SLAs Operations.”

IP SLAs integration with CFM gathers Ethernet layer statistical measurements by sending and receiving Ethernet data frames between CFM MEPs. Performance is measured between the source MEP and the destination MEP. Unlike other IP SLAs operations that provide performance metrics for only the IP layer, IP SLAs with CFM provides performance metrics for Layer 2.

You can manually configure individual Ethernet ping or jitter operations. You can also configure an IP SLAs automatic Ethernet operation that queries the CFM database for all MEPs in a given maintenance domain and VLAN. The operation then automatically creates individual Ethernet ping or jitter operations based on the discovered MEPs.

Because IP SLAs is a Cisco proprietary feature, interoperability between CFM draft 1 and CFM 802.1ag is handled automatically by the switch.

For more information about IP SLAs operation with CFM, see the *Configuring IP SLAs for Metro-Ethernet* feature module at this URL:

http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_metro_ethernet.html

Configuring Ethernet CFM

Configuring Ethernet CFM requires configuring the CFM domain. You can optionally configure and enable other CFM features such as crosschecking, remote MEP, port MEPs, SNMP traps, and fault alarms. Note that some of the configuration commands and procedures differ from those used in CFM draft 1.

Default Ethernet CFM Configuration

- 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.
- You cannot configure CFM on VLAN interfaces.

- CFM is supported on trunk ports, access ports, and 802.1Q tunnel ports with these exceptions:
  - Trunk ports configured as MEPs must belong to allowed VLANs
  - Access ports configured as MEPs must belong to the native VLAN.
- You can configure CFM and VLAN translation on the switch at the same time.
- CFM is not supported on private VLAN ports.
- A REP port or FlexLink port can also be a service (VLAN) MEP or MIP, but it cannot be a port MEP.
- CFM is supported on ports running STP.
- You must configure a port MEP at a lower level than any service (VLAN) MEPs on an interface.
- An 802.1Q (QinQ) tunnel port can be a CFM up MEP or a port MEP. On a Connected Grid switch, you can also configure a MEP on a selective QinQ port.
- A QinQ port cannot be a down MEP or a MIP; you can configure the port as a MIP, but it is not active or visible in traceroute. Port MEP frames received on a QinQ interface are not tunneled and are processed locally.
- On a QinQ port, ingress draft 1 traffic is tunneled without translation or consideration of CFM version.
- You cannot configure tunnel mode by using the native VLAN as the S-VLAN or the C-VLAN.
- For port MEP on a QinQ port, do not enter the **vlan dot1q tag native** global configuration command to enable tagging on native VLAN frames.
- Do not configure tagged or untagged 802.1ag CFM packets entering an 802.1Q tunnel port.
- Do not configure double-tagged 802.1ag CFM packets entering a trunk port.

Configuring the CFM Domain

Follow this procedure 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.

BEFORE YOU BEGIN

Review the "Information About Ethernet CFM" section on page 17-2 and "Ethernet CFM Configuration Guidelines" section on page 17-7.

DETAILED STEPS

Note You do not need to enter the **ethernet cfm ieee** global configuration command to configure the CFM version as 802.1ag. The CFM version is always 802.1ag and the command is automatically generated when you enable CFM.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ethernet cfm global**	Globally enable Ethernet CFM on the switch.

	Command	Purpose
Step 3	**ethernet cfm traceroute cache** [**size** *entries* | **hold-time** *minutes*]	(Optional) Configure the CFM traceroute cache. You can set a maximum cache size or hold time. • (Optional) For **size**, enter the cache size in number of entry lines. The range is from 1 to 4095; the default is 100 lines. • (Optional) For **hold-time**, enter the maximum cache hold time in minutes. The range is from 1 to 65535; the default is 100 minutes.
Step 4	**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.
Step 5	**ethernet cfm mip filter**	(Optional) Enable MIP filtering, which means that all CFM frames at a lower level are dropped. The default is disabled.
Step 6	**ethernet cfm domain** *domain-name* **level** *level-id*	Define a CFM domain, set the domain level, and enter ethernet-cfm configuration mode for the domain. The maintenance level number range is 0 to 7.
Step 7	**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.

	Command	Purpose
Step 8	**service** {*ma-name* | *ma-number* | *vpn-id vpn*} {**vlan** *vlan-id* [**direction down**] | **port**}	Define a customer service maintenance association (MA) name or number or VPN ID to be associated with the domain, a VLAN ID or port MEP, and enter ethernet-cfm-service configuration mode. • *ma-name*—a string of no more than 100 characters that identifies the MAID. • *ma-number*—a value from 0 to 65535. • *vpn-id vpn*—enter a VPN ID as the *ma-name*. • **vlan** *vlan-id*—VLAN range is from 1 to 4094. You cannot use the same VLAN ID for more than one domain at the same level. • (Optional) **direction down**—specify the service direction as down. • **port**—Configure port MEP, a down MEP that is untagged and not associated with a VLAN.
Step 9	**continuity-check**	Enable sending and receiving of continuity check messages.
Step 10	**continuity-check interval** *value*	(Optional) Set the interval at which continuity check messages are sent. The available values are 100 ms, 1 second, 10 seconds, 1 minute and 10 minutes. The default is 10 seconds. **Note** Because faster CCM rates are more CPU-intensive, we do not recommend configuring a large number of MEPs running at 100 ms intervals.
Step 11	**continuity-check loss-threshold** *threshold-value*	(Optional) Set the number of continuity check messages to be missed before declaring that an MEP is down. The range is 2 to 255; the default is 3.
Step 12	**maximum meps** *value*	(Optional) Configure the maximum number of MEPs allowed across the network. The range is from 1 to 65535. The default is 100.
Step 13	**sender-id** {**chassis** | **none**}	(Optional) Include the sender ID TLVs, attributes containing type, length, and values for neighbor devices. • **chassis**—Send the chassis ID (host name). • **none**—Do not include information in the sender ID.
Step 14	**mip auto-create** [**lower-mep-only** | **none**]	(Optional) Configure auto creation of MIPs for the service. • **lower-mep-only**—Create a MIP only if there is a MEP for the service in another domain at the next lower active level. • **none**—No MIP auto-create.
Step 15	**exit**	Return to ethernet-cfm configuration mode.

	Command	Purpose
Step 16	**mip auto-create [lower-mep-only]**	(Optional) Configure auto creation of MIPs for the domain. • **lower-mep-only**—Create a MIP only if there is a MEP for the service in another domain at the next lower active level.
Step 17	**mep archive-hold-time** *minutes*	(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.
Step 18	**exit**	Return to global configuration mode.
Step 19	**interface** *interface-id*	Specify an interface to configure, and enter interface configuration mode.
Step 20	**switchport mode trunk**	(Optional) Configure the port as a trunk port.
Step 21	**ethernet cfm mip level** *level-id*	(Optional) Configure a customer level or service-provider level maintenance intermediate point (MIP) for the interface. The MIP level range is 0 to 7. **Note** This step is not required if you have entered the **ethernet cfm mip auto-create** global configuration command or the **mip auto-create** ethernet-cfm or ethernet-cfm-srv configuration mode.
Step 22	**ethernet cfm mep domain** *domain-name* **mpid** *identifier* {**vlan** *vlan-id* | **port**}	Configure maintenance end points for the domain, and enter ethernet cfm mep mode. • **domain** *domain-name*—Specify the name of the created domain. • **mpid** *identifier*—Enter a maintenance end point identifier. The identifier must be unique for each VLAN (service instance). The range is 1 to 8191. • **vlan** *vlan-id*—Enter the service provider VLAN ID or IDs as a VLAN-ID (1 to 4094), a range of VLAN-IDs separated by a hyphen, or a series of VLAN IDs separated by comma. • **port**—Configure port MEP.
Step 23	**cos** *value*	(Optional) Specify the class of service (CoS) value to be sent with the messages. The range is 0 to 7.
Step 24	**end**	Return to privileged EXEC mode.
Step 25	**show ethernet cfm maintenance-points** {**local** | **remote**}	Verify the configuration.
Step 26	**show ethernet cfm errors [configuration]**	(Optional) Display the configuration error list.
Step 27	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** versions of the commands to remove the configuration or return to the default configurations.

EXAMPLE

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

BEFORE YOU BEGIN

Review the "Information About Ethernet CFM" section on page 17-2 and "Ethernet CFM Configuration Guidelines" section on page 17-7.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ethernet cfm mep crosscheck start-delay** *delay*	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	**ethernet cfm domain** *domain-name* **level** *level-id*	Define a CFM domain, set the domain level, and enter ethernet-cfm configuration mode for the domain. The maintenance level number range is 0 to 7.
Step 4	**service** {*ma-name* | *ma-number* | *vpn-id vpn*} {**vlan** *vlan-id*}	Define a customer service maintenance association name or number or VPN ID to be associated with the domain, and a VLAN ID, and enter ethernet-cfm-service configuration mode. • *ma-name*—a string of no more than 100 characters that identifies the MAID. • *ma-number*—a value from 0 to 65535. • *vpn-id 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.
Step 5	**mep mpid** *identifier*	Define the MEP maintenance end point identifier in the domain and service. The range is 1 to 8191.

	Command	Purpose
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**ethernet cfm mep crosscheck** {**enable** | **disable**} **domain** *domain-name* {**vlan** {*vlan-id* | **any**} | **port**}	Enable or disable CFM crosscheck for one or more VLANs or a port MEP in the domain. • **domain** *domain-name*—Specify the name of the created domain. • **vlan** {*vlan-id* | **any**}—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. Enter **any** for any VLAN. • **port**—Identify a port MEP.
Step 8	**show ethernet cfm maintenance-points remote crosscheck**	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.

EXAMPLE

The following example shows how to set the maximum number of seconds that a device will wait for remote MEPs to come up before the cross-check operation is started to 700:

```
Switch(config)# ethernet cfm mep crosscheck start-delay 700
```

The following example shows how to enable an Ethernet CFM MEP cross-check in CFM D1 at level 2 for VLAN IDs in the range from 3000 to 3375:

```
Switch# ethernet cfm mep crosscheck enable level 2 vlan 3000-3375
```

Configuring Static Remote MEP

BEFORE YOU BEGIN

Review the "Information About Ethernet CFM" section on page 17-2 and "Ethernet CFM Configuration Guidelines" section on page 17-7.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ethernet cfm domain** *domain-name* **level** *level-id*	Define a CFM domain, set the domain level, and enter ethernet-cfm configuration mode for the domain. The maintenance level number range is 0 to 7.
Step 3	**service** {*ma-name* | *ma-number* | *vpn-id vpn*} {**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 8191
Step 6	**continuity-check static rmep**	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.

EXAMPLE

```
Switch(config)# ethernet cfm domain CUSTOMER level 7
Switch(config-ecfm)# service test vlan 10
```

```
Switch(config-ecfm-srv)# continuity-check
Switch(config-ecfm-srv)# mep mpid 200
Switch(config-ecfm-srv)# continuity-check static rmep
Switch(config-ecfm-srv)# end
```

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.

BEFORE YOU BEGIN

Review the "Information About Ethernet CFM" section on page 17-2 and "Ethernet CFM Configuration Guidelines" section on page 17-7.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ethernet cfm domain** *domain-name* **level** *level-id*	Define a CFM domain, set the domain level, and enter ethernet-cfm configuration mode for the domain. The maintenance level number range is 0 to 7.
Step 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 vpn*—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 8191
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.

	Command	Purpose
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.
Step 12	**ethernet cfm mep domain** *domain-name* **mpid** *identifier* **port**	Configure the interface as a port MEP for the domain. • **domain** *domain-name*—Specify the name of the created domain. • **mpid** *identifier*—Enter a maintenance end point identifier. The identifier must be unique for each VLAN (service instance). The range is 1 to 8191.
Step 13	**end**	Return to privileged EXEC mode.
Step 14	**show ethernet cfm maintenance-points remote static**	Verify the configuration.
Step 15	**show ethernet cfm errors** [**configuration**]	Enter this command after you enable CFM crosscheck to display the results of the crosscheck operation. Enter the **configuration** keyword to display the configuration error list.
Step 16	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of each command to remove a configuration or to return to the default settings.

This is a sample configuration for a port MEP:

```
Switch(config)# ethernet cfm domain abc level 3
Switch(config-ecfm)# service PORTMEP port
Switch(config-ecfm-srv)# mep mpid 222
Switch(config-ecfm-srv)# continuity-check
Switch(config-ecfm-srv)# continuity-check static rmep
Switch(config-ecfm-srv)# exit
Switch(config-ecfm)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ethernet cfm mep domain abc mpid 111 port
Switch(config-if)# end
```

Configuring SNMP Traps

BEFORE YOU BEGIN

Review the "Information About Ethernet CFM" section on page 17-2 and "Ethernet CFM Configuration Guidelines" section on page 17-7.

DETAILED STEPS

	Command	Purpose
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.

EXAMPLE

```
Switch(config)# snmp-server enable traps ethernet cfm cc mep-up mep-down config loop
cross-connect
```

Configuring Fault Alarms

You can configure Ethernet CFM fault alarms in either global configuration mode or Ethernet CFM interface MEP mode. In case of conflict, the interface MEP mode configuration takes precedence.

BEFORE YOU BEGIN

Review the "Information About Ethernet CFM" section on page 17-2 and "Ethernet CFM Configuration Guidelines" section on page 17-7.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
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 (service instance). The range is 1 to 8191. • **vlan** *vlan-id*—Enter the service provider VLAN ID or IDs as a VLAN-ID (1 to 4094), a range of VLAN-IDs separated by a hyphen, or a series of VLAN IDs separated by comma.
Step 8	**ethernet cfm alarm notification** {**all** | **error-xcon** | **mac-remote-error-xcon** | **none** | **remote-error-xcon** | **xcon**}	(Optional) Enable Ethernet CFM fault alarm notification for the specified defects on the interface. **Note** The Ethernet CFM interface MEP alarm configuration takes precedence over the global configuration.

	Command	Purpose
Step 9	**ethernet cfm alarm** {**delay** *value* | **reset** *value*}	(Optional) Set an alarm delay period or a reset period. **Note** The Ethernet CFM interface MEP alarm configuration takes precedence over the global configuration.
Step 10	**end**	Return to privileged EXEC mode.
Step 11	**show running-config**	Verify your entries.
Step 12	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of each command to remove a configuration or to return to the default settings.

EXAMPLE

The following example shows how to set up notification for all defects:

```
Switch(config)# ethernet cfm alarm notification all
```

The following example shows how to set the time during which one or more defects must be present before a fault alarm is issued to 5000 ms:

```
Switch(config)# ethernet cfm alarm delay 5000
```

Configuring IP SLAs CFM Operation

You can manually configure an individual IP SLAs Ethernet ping or jitter echo operation or you can configure IP SLAs Ethernet operation with endpoint discovery. You can also configure multiple operation scheduling. For accurate one-way delay statistics, the clocks on the endpoint switches must be synchronized. You can configure the endpoint switches with Network Time Protocol (NTP) so that the switches are synchronized to the same clock source.

For more information about configuring IP SLAs, see Chapter 16, "Configuring Cisco IOS IP SLAs Operations."

This section includes the following topics:

- Manually Configuring an IP SLAs CFM Probe or Jitter Operation, page 17-19
- Configuring an IP SLAs Operation with Endpoint Discovery, page 17-22

Manually Configuring an IP SLAs CFM Probe or Jitter Operation

BEFORE YOU BEGIN

Review the "Information About Ethernet CFM" section on page 17-2 and "Ethernet CFM Configuration Guidelines" section on page 17-7.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip sla** *operation-number*	Create an IP SLAs operation, and enter IP SLAs configuration mode.
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 (service instance). The range is 1 to 8191. • 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 (ms0 for calculating network monitoring statistics. The range is 0 to 2147483647; the default is 5000.

	Command	Purpose
Step 11	**timeout** *milliseconds*	(Optional) Specify the amount of time in ms that the IP SLAs operation waits for a response from its request packet. The range is 0 to 604800000; the default value is 5000.
Step 12	**exit**	Return to global configuration mode.
Step 13	**ip sla schedule** *operation-number* [**ageout** *seconds*] [**life** {**forever** | *seconds*}] [**recurring**] [**start-time** {*hh:mm* {*:ss*} [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*}]	Schedule the time parameters for the IP SLAs operation. • *operation-number*—Enter the IP SLAs operation number. • (Optional) **ageout** *seconds*—Enter the number of seconds to keep the operation in memory when it is not actively collecting information. The range is 0 to 2073600 seconds. The default is 0 seconds. • (Optional) **life**—Set the operation to run indefinitely (**forever**) or for a specific number of *seconds*. The range is from 0 to 2147483647. The default is 3600 seconds (1 hour). • (Optional) **recurring**—Set the probe to be automatically scheduled every day. • (Optional) **start-time**—Enter the time for the operation to begin collecting information: – To start at a specific time, enter the hour, minute, second (in 24-hour notation), and day of the month. – Enter **pending** to select no information collection until a start time is selected. – Enter **now** to start the operation immediately. – Enter **after** *hh:mm:ss* to show that the operation should start after the entered time has elapsed.
Step 14	**end**	Return to privileged EXEC mode.
Step 15	**show ip sla configuration** [*operation-number*]	Show the configured IP SLAs operation.
Step 16	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To remove an IP SLAs operation, enter the no **ip sla** *operation-number* global configuration command.

EXAMPLE

```
Switch(config)# ip sla 1
Switch(config-ip-sla)# ethernet echo mpid 222 domain abc vlan 10
Switch(config-ip-sla)# exit
Switch(config)# ip sla schedule 1 start-time after 00:05:00
Switch(config)# end
```

Configuring an IP SLAs Operation with Endpoint Discovery

Follow this procedure 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.

BEFORE YOU BEGIN

Review the "Information About Ethernet CFM" section on page 17-2 and "Ethernet CFM Configuration Guidelines" section on page 17-7.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip sla ethernet-monitor** *operation-number*	Begin configuration of an IP SLAs automatic Ethernet operation, and enter IP SLAs Ethernet monitor configuration mode.
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 8191. • 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.

	Command	Purpose
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.
Step 11	**ip sla schedule** *operation-number* [**ageout** *seconds*] [**life** {**forever** | *seconds*}] [**recurring**] [**start-time** {*hh:mm* {*:ss*} [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*}]	Schedule the time parameters for the IP SLAs operation. • *operation-number*—Enter the IP SLAs operation number. • (Optional) **ageout** *seconds*—Enter the number of seconds to keep the operation in memory when it is not actively collecting information. The range is 0 to 2073600 seconds. The default is 0 seconds. • (Optional) **life**—Set the operation to run indefinitely (**forever**) or for a specific number of *seconds*. The range is from 0 to 2147483647. The default is 3600 seconds (1 hour). • (Optional) **recurring**—Set the probe to be automatically scheduled every day. • (Optional) **start-time**—Enter the time for the operation to begin collecting information: – To start at a specific time, enter the hour, minute, second (in 24-hour notation), and day of the month. – Enter **pending** to select no information collection until a start time is selected. – Enter **now** to start the operation immediately. – Enter **after** *hh:mm:ss* to show that the operation should start after the entered time has elapsed.
Step 12	**end**	Return to privileged EXEC mode.
Step 13	**show ip sla configuration** [*operation-number*]	Show the configured IP SLAs operation.
Step 14	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To remove an IP SLAs operation, enter the **no ip sla** *operation-number* global configuration command.

EXAMPLE

```
Switch(config)# ip sla ethernet-monitor 3
Switch(config-ip-sla-ethernet-monitor)# type jitter domain testdomain vlan 20
Switch(config-ip-sla-ethernet-monitor)# exit
Switch(config)# ip sla schedule 1 start-time now life forever
Switch(config)# end
```

Information About CFM ITU-T Y.1731 Fault Management

The ITU-T Y.1731 feature provides new CFM functionality for fault and performance management for service providers in large network. The switch supports Ethernet Alarm Indication Signal (ETH-AIS), Ethernet Remote Defect Indication (ETH-RDI), Ethernet Locked Signal (ETH-LCK), and Ethernet Multicast Loopback Message (MCAST-LBM) functionality for fault detection, verification, and isolation.

Y.1731 Terminology

- Server MEP—the combination of the server layer termination function and server or Ethernet adaptation layer termination function or server or Ethernet adaptation function, where the server layer termination function is expected to run OAM mechanisms specific to the server layer. The supported mechanisms are link up, link down, and 802.3ah.
- Server layer—a virtual MEP layer capable of detecting fault conditions.
- Defect conditions:
  - Loss of continuity (LOC): the MEP stopped receiving CCM frames from a peer MEP.
  - Mismerge: the MEP received a CCM frame with a correct maintenance level (matching the MEP level) but an incorrect maintenance ID.
  - Unexpected MEP: the MEP received a CCM frame with the correct maintenance level (matching the MEP's level) and correct maintenance ID, but an unexpected MEP ID.
  - Unexpected maintenance level: the MEP received a CCM frame with an incorrect maintenance level.
  - Unexpected period: the MEP received a CCM frame with a correct maintenance level, a correct maintenance ID, a correct MEP ID, but a different transmission period field.
- Signal fail—the MEP declares a signal fail condition when it detects a defect condition.
- Alarm Indication Signal (AIS) condition—the MEP received an AIS frame.
- Remote Defect Indication (RDI) condition—The MEP received a CCM frame with the RDI field set.
- Locked Signal (LCK) condition—The MEP received an LCK frame.

Alarm Indication Signals

The Ethernet Alarm Signal function (ETH-AIS) is used to suppress alarms after defects are detected at the *server* (sub) layer, which is a virtual MEP layer capable of detecting fault conditions. A fault condition could be a signal fail condition, an AIS condition, or a LCK condition.

Note Although the configuration is allowed, you should not configure AIS in networks running STP. An STP configuration might cause AIS interruption or redirection.

When a MEP or a service MEP (SMEP) detects a connectivity fault at a specific maintenance association level, it multicasts AIS frames in the direction away from the detected failure at the client maintenance association level. The frequency of AIS frame transmission is based on the AIS transmission period. The first AIS frame is always sent immediately following the detection of the defect condition. We recommend a transition period of 1 second in a network of only a few VLANs to ensure that the first AIS frame is sent immediately following error detection. We recommend a 60-second interval in a network of mulltiple (up to 4094) VLANs to prevent stressing the network with 1-second transmissions.

A MEP that receives a frame with ETH-AIS information cannot determine the specific server with the defect condition or the set of peer MEPs for which it should suppress alarms. Therefore, it suppresses alarms for all peer MEPs, whether or not they are connected.

When a MEP receives an AIS frame, it examines it to be sure that the Maintenance Entity Group (MEG) level matches its own MEG and then detects the AIS default condition. (A MEG is Y.1731 terminology for maintenance association in 802.1ag.) After this detection, if no AIS frames are received for an interval of 3.5 times the AIS transmission period, the MEP clears the AIS defect condition. For example, if the AIS timer is set for 60 seconds, the AIS timer period expires after 3.5 times 60, or 210 seconds.

The AIS condition is terminated when a valid CCM is received with all error conditions cleared or when the AIS period timer expires (the default time is 60 seconds).

Ethernet Remote Defect Indication

When Ethernet OAM continuity check (ETH-CC) transmission is enabled, the Ethernet Remote Defect Indication (ETH-RDI) function uses a bit in the CFM CC message to communicate defect conditions to the MEP peers. For ETH-RDI functionality, you must configure the MEP MEG level, the ETH-CC transmission period, and the ETH-CC frame priority. ETH-RDI does not require any MIP configuration.

When a MEP receives frames with ETH-RDI information, it determines that its peer MEP has encountered a defect condition and sets the RDI files in the CCM frames for the duration of the defect condition. When the defect condition clears, the MEP clears the RDI field.

When a MEP receives a CCM frame, it examines it to ensure that its MEG level is the same and if the RDI field is set, it detects an RDI condition. For point-to-point Ethernet connections, a MEP can clear the RDI condition when it receives the first frame from its peer MEP with the RDI field cleared. However, for multipoint Ethernet connectivity, the MEP cannot determine the associated subset of peer MEPs with which the sending MEP has seen the defect condition. It can clear the RDI condition after it receives CCM frames with the RDI field cleared from its entire list of peer MEPs.

Ethernet Locked Signal

The Ethernet Locked Signal (ETH-LCK) function communicates the administrative locking of a server MEP and interruption of data traffic being forwarded to the MEP expecting the traffic. A MEP that receives frames with ETH-LCK information can differentiate between a defect condition and an administrative locking. ETH-LCK relies on loopback information (local, remote, port loopback, per-VLAN loopback, and terminal loopback). The default timer for ETH-LCK is 60 seconds and the default level is the MIP level.

When a MEP is administratively locked, it sends LCK frames in a direction opposite to its peer MEPs, based on the LCK transmission period, which is the same as the AIS transmission period. The first LCK frame is sent immediately following the administrative or diagnostic action.

A MEP receiving a LCK frame verifies that the maintenance level matches its configured maintenance level, and detects a LCK condition. When no LCK frames are received for an interval of 3.5 times the LCK transmission period, the MEP clears the LCK condition.

Multicast Ethernet Loopback

The multicast Ethernet loopback (ETH-LB) function verifies bidirectional connectivity of a MEP with its peer MEPs and is an on-demand OAM function. When the feature is invoked on a MEP by entering the **ping** privileged EXEC command, the MEP sends a multicast frame with ETH-LB request information to peer MEPs in the same MEG. The MEP expects to receive a unicast frame with ETH-LB reply information from its peer MEPs within a specified time period. A MEP receiving a multicast frame with ETH-LB request information validates the frame and transmits a frame with reply information.

To configure multicast ETH-LB, you configure the MEG level of the MEP and the priority of the multicast frames with ETH-LB requests. Multicast frames with ETH-LB request information are always marked as drop ineligible. No MIP configuration is required.

The MEP sends multicast LB message frames on an on-demand basis. After sending a multicast LBM frame, the MEP expects to receive LB reply frames within 5 seconds.

When a MEP receives a valid LBM frame, it generates an LB reply frame and sends it to the requested MEP after a random delay in the range of 0 to 1 second. The validity of the frame is determined on its having the correct MEG level.

When a MEP sends a multicast LBM frame and receives an LB reply frame within 5 seconds, the LB reply frame is valid.

Configuring Y.1731 Fault Management

To configure Y.1731 fault management, you must enable CFM and configure MIPs on the participating interfaces. AIS messages are generated only on interfaces with a configured MIP.

Default Y.1731 Configuration

- ETH-AIS and ETH-LCK are enabled by default when CFM is enabled.
- When you configure ETH-AIS or ETH-LCK, you must configure CFM before ETH-AIS or ETH-LCK is operational.
- ETH-RDI is set automatically when continuity check messages are enabled.

Configuring ETH-AIS

BEFORE YOU BEGIN

Review the "Information About CFM ITU-T Y.1731 Fault Management" section on page 17-24.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ethernet cfm ais link-status global**	Configure AIS-specific SMEP commands by entering config-ais-link-cfm mode.
Step 3	**level** *level-id* or disable	Configure the maintenance level for sending AIS frames transmitted by the SMEP. The range is 0 to 7. or Disable generation of ETH-AIS frames.
Step 4	**period** *value*	Configure the SMEP AIS transmission period interval. Allowable values are 1 second or 60 seconds.
Step 5	**exit**	Return to global configuration mode.
Step 6	**ethernet cfm domain** *domain-name* **level** *level-id*	Define a CFM domain, set the domain level, and enter ethernet-cfm configuration mode for the domain. The maintenance level number range is 0 to 7.

	Command	Purpose
Step 7	**service** {*ma-name* | *ma-number* | *vpn-id vpn*} {**vlan** *vlan-id* [**direction down**] | **port**}	Define a customer service maintenance association (MA) name or number to be associated with the domain, or a VLAN ID or VPN-ID, and enter ethernet-cfm-service configuration mode. • *ma-name*—a string of no more than 100 characters that identifies the MAID. • *ma-number*—a value from 0 to 65535. • *vpn-id*—enter a VPN ID as the *ma-name*. • **vlan** *vlan-id*—VLAN range is from 1 to 4094. You cannot use the same VLAN ID for more than one domain at the same level. • (Optional) **direction down**—specify the service direction as down. • **port**—Configure port MEP, which is a down MEP that is untagged and not associated with a VLAN.
Step 8	**ais level** *level-id*	(Optional) Configure the maintenance level for sending AIS frames transmitted by the MEP. The range is 0 to 7.
Step 9	**ais period** *value*	(Optional) Configure the MEP AIS transmission period interval. Allowable values are 1 second or 60 seconds.
Step 10	**ais expiry-threshold** *value*	(Optional) Set the expiring threshold for the MA as an integer. The range is 2 to 255. The default is 3.5.
Step 11	**no ais suppress-alarms**	(Optional) Override the suppression of redundant alarms when the MEP goes into an AIS defect condition after receiving an AIS message.
Step 12	**exit**	Return to ethernet-cfm configuration mode.
Step 13	**exit**	Return to global configuration mode.
Step 14	**interface** *interface-id*	Specify an interface ID, and enter interface configuration mode.
Step 15	[**no**] **ethernet cfm ais link-status**	Enable or disable sending AIS frames from the SMEP on the interface.
Step 16	**ethernet cfm ais link-status period** *value*	Configure the ETH-AIS transmission period generated by the SMEP on the interface. Allowable values are 1 second or 60 seconds.
Step 17	**ethernet cfm ais link-status level** *level-id*	Configure the maintenance level for sending AIS frames transmitted by the SMEP on the interface. The range is 0 to 7.
Step 18	**end**	Return to privileged EXEC mode.
Step 19	**show ethernet cfm smep** [**interface** *interface-id*]	Verify the configuration.

	Command	Purpose
Step 20	**show ethernet cfm error**	Display received ETH-AIS frames and other errors.
Step 21	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the commands to return to the default configuration or to remove a configuration. To disable the generation of ETH-AIS frames, enter the **disable** config-ais-link-cfm mode command.

EXAMPLE

This is an example of the output from the **show ethernet cfm smep** command when Ethernet AIS has been enabled:

```
Switch# show ethernet cfm smep
SMEP Settings:
--------------
Interface: GigabitEthernet0/3
LCK-Status: Enabled
LCK Period: 60000 (ms)
Level to transmit LCK: Default
AIS-Status: Enabled
AIS Period: 60000 (ms)
Level to transmit AIS: Default
Defect Condition: AIS
```

Configuring ETH-LCK

BEFORE YOU BEGIN

Review the "Information About CFM ITU-T Y.1731 Fault Management" section on page 17-24.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ethernet cfm lck link-status global**	Configure SMEP LCK commands by entering config-lck-link-cfm mode.
Step 3	**level** *level-id* or disable	Configure the maintenance level for sending ETH-LCK frames transmitted by the SMEP. The range is 0 to 7. or Disable generation of ETH-LCK frames.
Step 4	**period** *value*	Configure the SMEP ETH-LCK frame transmission period interval. Allowable values are 1 second or 60 seconds.
Step 5	**exit**	Return to global configuration mode.

	Command	Purpose
Step 6	**ethernet cfm domain** *domain-name* **level** *level-id*	Define a CFM domain, set the domain level, and enter ethernet-cfm configuration mode for the domain. The maintenance level number range is 0 to 7.
Step 7	**service** {*ma-name* | *ma-number* | *vpn-id vpn*} {**vlan** *vlan-id* [**direction down**] | **port**}	Define a customer service maintenance association name or number to be associated with the domain, or a VLAN ID or VPN-ID, and enter ethernet-cfm-service configuration mode. • *ma-name*—a string of no more than 100 characters that identifies the MAID. • *ma-number*—a value from 0 to 65535. • *vpn-id*—enter a VPN ID as the *ma-name*. • **vlan** *vlan-id*—VLAN range is from 1 to 4094. You cannot use the same VLAN ID for more than one domain at the same level. • (Optional) **direction down**—specify the service direction as down. • **port**—Configure port MEP, a down MEP that is untagged and not associated with a VLAN.
Step 8	**lck level** *level-id*	(Optional) Configure the maintenance level for sending ETH-LCK frames sent by the MEP. The range is 0 to 7.
Step 9	**lck period** *value*	(Optional) Configure the MEP ETH-LCK frame transmission period interval. Allowable values are 1 second or 60 seconds.
Step 10	**lck expiry-threshold** *value*	(Optional) Set the expiring threshold for the MA. The range is 2 to 255. The default is 3.5.
Step 11	**exit**	Return to ethernet-cfm configuration mode.
Step 12	**exit**	Return to global configuration mode.
Step 13	**interface** *interface-id*	Specify an interface ID, and enter interface configuration mode.
Step 14	[**no**] **ethernet cfm lck link-status**	Enable or disable sending ETH-LCK frames from the SMEP on the interface.
Step 15	**ethernet cfm lck link-status period** *value*	Configure the ETH-LCK transmission period generated by the SMEP on the interface. Allowable values are 1 second or 60 seconds.
Step 16	**ethernet cfm lck link-status level** *level-id*	Configure the maintenance level for sending ETH-LCK frames sent by the SMEP on the interface. The range is 0 to 7.
Step 17	**end**	Return to privileged EXEC mode.

	Command	Purpose
Step 18	**ethernet cfm lck start mpid** *local-mpid* **domain** *domain-name* **vlan** *vlan-id* [**drop l2-bpdu**]	(Optional) Put a MEP in LCK condition. • The **mpid** *local-mpid* **domain** *domain-name* **vlan** *vlan-id* identify the MEP. • (Optional) **drop l2-bpdu** specifies that the switch should drop all data frames, all Layer 3 control traffic, and all Layer 2 BPDUs except CFM frames for that MEP. If not entered, the switch drops only data frames and Layer 3 control frames.
Step 19	**ethernet cfm lck start interface** *interface-id* **direction** {**up** | **down**} [**drop l2-bpdu**]	(Optional) Put an interface in LCK condition. • **interface** *interface-id*—Specify the interface to be put in LCK condition. • **direction inward**—The LCK is in the direction toward the relay; that is, within the switch. • **direction outward**—The LCK is in the direction of the wire. • (Optional) **drop l2-bpdu** specifies that all Layer 2 BPDUs except CFM frames, all data frames, and all Layer 3 control traffic are dropped for that MEP. If not entered, only data frames and Layer 3 control frames are dropped.
Step 20	**show ethernet cfm smep** [**interface** *interface-id*]	Verify the configuration.
Step 21	**show ethernet cfm error**	Display received ETH-LCK frames.
Step 22	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To put a MEP out of LCK condition, enter the **ethernet cfm lck stop mpid** *local-mpid* **domain** *domain-name* **vlan** *vlan-id* privileged EXEC command. To put an interface out of LCK condition, enter the **ethernet cfm lck start interface** *interface-id* **direction** {**inward** | **outward**} privileged EXEC command.

EXAMPLE

This is an example of the output from the **show ethernet cfm smep** command when Ethernet LCK has been enabled:

```
Switch# show ethernet cfm smep
SMEP Settings:
--------------
Interface: GigabitEthernet0/3
LCK-Status: Enabled
LCK Period: 60000 (ms)
Level to transmit LCK: Default
AIS-Status: Enabled
AIS Period: 60000 (ms)
Level to transmit AIS: Default
Defect Condition: AIS
```

Using Multicast Ethernet Loopback

You can use the **ping** privileged EXEC command to verify bidirectional connectivity of a MEP, as in this example:

```
Switch# ping ethernet multicast domain CD vlan 10
Type escape sequence to abort.
Sending 5 Ethernet CFM loopback messages to 0180.c200.0037, timeout is 5 seconds:
Reply to Multicast request via interface FastEthernet1/0/3, from 001a.a17e.f880, 8 ms
Total Loopback Responses received: 1
```

Managing and Displaying Ethernet CFM Information

You can use the privileged EXEC commands in the following table to clear Ethernet CFM information:

Command	Purpose
clear ethernet cfm ais domain *domain-name* **mpid** *id* {**vlan** *vlan-id* | **port**}	Clear MEPs with matching domain and VLAN ID out of AIS defect condition.
clear ethernet cfm ais link-status interface *interface-id*	Clear a SMEP out of AIS defect condition.
clear ethernet cfm error	Clear all CFM error conditions, including AIS.

You can use the privileged EXEC commands in the following table to display Ethernet CFM information:

Command	Purpose
show ethernet cfm domain [**brief**]	Displays CFM domain information or brief domain information.
show ethernet cfm errors [**configuration | domain-id**]	Displays CFM continuity check error conditions logged on a device since it was last reset or the log was last cleared. When CFM crosscheck is enabled, displays the results of the CFM crosscheck operation.
show ethernet cfm maintenance-points local [detail | domain | interface | level | mep | mip]	Displays maintenance points configured on a device.
show ethernet cfm maintenance-points remote [**crosscheck | detail | domain | static**]	Displays information about a remote maintenance point domains or levels or details in the CFM database.
show ethernet cfm mpdb	Displays information about entries in the MIP continuity-check database.
show ethernet cfm smep [**interface** *interface-id*]	Displays Ethernet CFM SMEP information.
show ethernet cfm traceroute-cache	Displays the contents of the traceroute cache.
show platform cfm	Displays platform-independent CFM information.

EXAMPLE

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     100Total 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
     MAName                                     Reason                 Age
----------------------------------------------------------------------------------
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
------------------------------------------------------------------------------
 Level Port           MacAddress     SrvcInst   Type    Id
------------------------------------------------------------------------------
*5     Gi0/3          0021.d7ef.0700 N/A        Vlan    2,7
```

This is an example of output from the **show ethernet cfm traceroute** command:

```
Switch# show ethernet cfm traceroute
Current Cache-size: 0 Hops
Max Cache-size: 100 Hops
```

```
Hold-time: 100 Minutes
```

You can use the privileged EXEC commands in the following table to display IP SLAs Ethernet CFM information:

Command	Purpose
show ip sla configuration [*entry-number*]	Displays configuration values including all defaults for all IP SLAs operations or a specific operation.
show ip sla ethernet-monitor configuration [*entry-number*]	Displays the configuration of the IP SLAs automatic Ethernet operation.
show ip sla statistics [*entry-number* | **aggregated** | **details**]	Display current or aggregated operational status and statistics.

Information About the Ethernet OAM Protocol

The Ethernet OAM protocol for installing, monitoring, and troubleshooting Metro Ethernet networks and Ethernet WANs relies on an optional sublayer in the data link layer of the OSI model. Normal link operation does not require Ethernet OAM. You can implement Ethernet OAM on any full-duplex point-to-point or emulated point-to-point Ethernet link for a network or part of a network (specified interfaces).

OAM frames, called OAM protocol data units (OAM PDUs) use the slow protocol destination MAC address 0180.c200.0002. They are intercepted by the MAC sublayer and cannot propagate beyond a single hop within an Ethernet network. Ethernet OAM is a relatively slow protocol, with a maximum transmission rate of 10 frames per second, resulting in minor impact to normal operations. However, when you enable link monitoring, because the CPU must poll error counters frequently, the number of required CPU cycles is proportional to the number of interfaces that must be polled.

Ethernet OAM has two major components:

- The OAM client establishes and manages Ethernet OAM on a link and enables and configures the OAM sublayer. During the OAM discovery phase, the OAM client monitors OAM PDUs received from the remote peer and enables OAM functionality. After the discovery phase, it manages the rules of response to OAM PDUs and the OAM remote loopback mode.
- The OAM sublayer presents two standard 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 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.

Note Another way to test connectivity and ensure that a remote device is reachable is to configure Ethernet loopback. See the "Enabling Ethernet Loopback" section on page 17-47.

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.

Configuring Ethernet OAM

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

BEFORE YOU BEGIN

Review the "Information About the Ethernet OAM Protocol" section on page 17-34.

DETAILED STEPS

	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.
Step 3	**ethernet oam**	Enable Ethernet OAM on the interface.

	Command	Purpose
Step 4	**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.

EXAMPLE

The following example shows how to activate an Ethernet OAM interface that was previously configured to be in passive mode:

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# ethernet oam mode active
```

The following example shows how to set the maximum transmission rate of OAM PDUs on interface GigabitEthernet 0/1 to 5 transmissions per second:

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# ethernet oam max-rate 5
```

The following example shows how to set the timeout period to 25 seconds on interface GigabitEthernet 0/1:

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# ethernet oam timeout 25
```

Enabling Ethernet OAM Remote Loopback

You must enable Ethernet OAM remote loopback on an interface for the local OAM client to initiate OAM remote loopback operations. Changing this setting causes the local OAM client to exchange configuration information with its remote peer. Remote loopback is disabled by default.

Remote loopback has these limitations:

- Internet Group Management Protocol (IGMP) packets are not looped back.
- You cannot configure Ethernet OAM remote loopback on ISL ports or ports that belong to an EtherChannel.
- If dynamic ARP inspection is enabled, ARP or reverse ARP packets are not looped or dropped.

BEFORE YOU BEGIN

Review the "Information About the Ethernet OAM Protocol" section on page 17-34.

DETAILED STEPS

	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.
Step 3	**ethernet oam remote-loopback** {**supported** | **timeout** *seconds*}	Enable Ethernet remote loopback on the interface, or set a loopback timeout period. • Enter **supported** to enable remote loopback. • Enter **timeout** *seconds* to set a remote loopback timeout period. The range is from 1 to 10 seconds.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**ethernet oam remote-loopback** {**start** | **stop**} {**interface** *interface-id*}	Turn on or turn off Ethernet OAM remote loopback on an interface.
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.

Use the **no ethernet oam remote-loopback** {**supported** | **timeout**} interface configuration command to disable remote loopback support or to remove the timeout setting.

EXAMPLE

The following example shows how to enable remote loopback support on interface GigabitEthernet 2/1:

```
Switch(config)# interface gigabitethernet 2/1
Switch(config-if)# ethernet oam remote-loopback supported
```

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.

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.

BEFORE YOU BEGIN

Review the "Information About the Ethernet OAM Protocol" section on page 17-34.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Define an interface, and enter interface configuration mode.
Step 3	**ethernet oam link-monitor supported**	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 **no ethernet oam link-monitor supported** command.
Step 4	**ethernet oam link-monitor symbol-period** {**threshold** {**high** {*high symbols*	**none**}	**low** {*low-symbols*}}	**window** *symbols*} **Note** Repeat this step to configure both high and low thresholds.	(Optional) Configure high and low thresholds for an error-symbol period that trigger an error-symbol period link event. • Enter **threshold high** *high-symbols* to set a high threshold in number of symbols. The range is 1 to 65535. 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-symbols* to set a low threshold in number of symbols. The range is 0 to 65535. It must be lower than the high threshold. • Enter **window** *symbols* to set the window size (in number of symbols) of the polling period. The range is 1 to 65535 symbols.

	Command	Purpose
Step 5	**ethernet oam link-monitor frame** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *milliseconds*} **Note** Repeat this step to configure both high and low thresholds.	(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. 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 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 multiples of 100. The default is 100.
Step 6	**ethernet oam link-monitor frame-period** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *frames*} **Note** Repeat this step to configure both high and low thresholds.	(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. 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 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.

	Command	Purpose
Step 7	**ethernet oam link-monitor frame-seconds** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *milliseconds*} **Note** Repeat this step to configure both high and low thresholds.	(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 a polling window size in number of milliseconds. The range is 100 to 9000; each value is a multiple of 100 milliseconds. The default is 1000.
Step 8	**ethernet oam link-monitor receive-crc** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *milliseconds*} **Note** Repeat this step to configure both high and low thresholds.	(Optional) Configure thresholds for monitoring ingress frames received with cyclic redundancy code (CRC) errors for a period of time. • Enter **threshold high** *high-frames* to set a high threshold for the number of frames received with CRC errors. The range is 1 to 65535 frames. • Enter **threshold high none** to disable the high threshold. • Enter **threshold low** *low-frames* to set a low threshold in number of frames. The range is 0 to 65535. The default is 1. • Enter **window** *milliseconds* to set the a window and period of time during which frames with CRC errors are counted. The range is 10 to 1800 and represents the number of milliseconds in multiples of 100. The default is 100.
Step 9	[**no**] **ethernet link-monitor on**	(Optional) Start or stop (when the **no** keyword is entered) link-monitoring operations on the interface. Link monitoring operations start automatically when support is enabled.
Step 10	**end**	Return to privileged EXEC mode.
Step 11	**show ethernet oam status** [**interface** *interface-id*]	Verify the configuration.
Step 12	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Enter the **no** form of the commands to disable the configuration. Use the **no** form of each command to disable the threshold setting.

EXAMPLE

```
Switch(config)# interface gigabitEthernet 3/8
Switch(config-if)#
Switch(config-if)# ethernet oam

Switch(config-if)# ethernet oam link-monitor symbol-period threshold high 299
Switch(config-if)# ethernet oam link-monitor frame window 399
Switch(config-if)# ethernet oam link-monitor frame-period threshold high 599
Switch(config-if)# ethernet oam link-monitor frame-seconds window 699
Switch(config-if)# ethernet oam link-monitor receive-crc window 99
Switch(config-if)# exit
```

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.

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. The switch can also respond to and generate Dying Gasp PDUs based on loss of power.

BEFORE YOU BEGIN

Review the "Information About the Ethernet OAM Protocol" section on page 17-34.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Define an interface, and enter interface configuration mode.
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.

	Command	Purpose
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.

Enter the **no ethernet remote-failure** {**critical-event** | **dying-gasp** | **link-fault**} **action** command to disable the remote failure indication action.

EXAMPLE

```
Switch(config)# interface gigabitEthernet 3/8
Switch(config-if)#
Switch(config-if)# ethernet oam

Switch(config-if)# ethernet oam remote-failure dying-gasp action error-disable-interface
Switch(config-if)# end
```

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.

The switch does not support monitoring egress frames with CRC errors. 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 can enter it, but it is not supported.

BEFORE YOU BEGIN

Review the "Information About the Ethernet OAM Protocol" section on page 17-34.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**template** *template-name*	Create a template, and enter template configuration mode.

	Command	Purpose
Step 3	**ethernet oam link-monitor receive-crc** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *milliseconds*}	(Optional) Configure thresholds for monitoring ingress frames received with cyclic redundancy code (CRC) errors for a period of time. • Enter **threshold high** *high-frames* to set a high threshold for the number of frames received with CRC errors. The range is 1 to 65535 frames. • Enter **threshold high none** to disable the high threshold. • Enter **threshold low** *low-frames* to set a low threshold in number of frames. The range is 0 to 65535. The default is 1. • Enter **window** *milliseconds* to set the a window and period of time during which frames with CRC errors are counted. The range is 10 to 1800 and represents the number of milliseconds in multiples of 100. The default is 100.
Step 4	**ethernet oam link-monitor symbol-period** {**threshold** {**high** {*high symbols* | **none**} | **low** {*low-symbols*}} | **window** *symbols*}	(Optional) Configure high and low thresholds for an error-symbol period that triggers an error-symbol period link event. • Enter **threshold high** *high-symbols* to set a high threshold in number of symbols. The range is 1 to 65535. • Enter **threshold high none** to disable the high threshold. • Enter **threshold low** *low-symbols* to set a low threshold in number of symbols. The range is 0 to 65535. It must be lower than the high threshold. • Enter **window** *symbols* to set the window size (in number of symbols) of the polling period. The range is 1 to 65535 symbols.

	Command	Purpose
Step 5	**ethernet oam link-monitor frame** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *milliseconds*}	(Optional) Configure high and low thresholds for error frames that trigger an error-frame link event. • Enter **threshold high** *high-frames* to set a high threshold in number of frames. The range is 1 to 65535. You must enter a high threshold. • Enter **threshold high none** to disable the high threshold. • Enter **threshold low** *low-frames* to set a low threshold in number of frames. The range is 0 to 65535. The default is 1. • Enter **window** *milliseconds* to set the a window and period of time during which error frames are counted. The range is 10 to 600 and represents the number of milliseconds in a multiple of 100. The default is 100.
Step 6	**ethernet oam link-monitor frame-period** {**threshold** {**high** {*high-frames* | **none**} | **low** {*low-frames*}} | **window** *frames*}	(Optional) Configure high and low thresholds for the error-frame period that triggers an error-frame-period link event. • Enter **threshold high** *high-frames* to set a high threshold in number of frames. The range is 1 to 65535. You must enter a high threshold. • Enter **threshold high none** to disable the high threshold. • Enter **threshold low** *low-frames* to set a low threshold in number of frames. The range is 0 to 65535. The default is 1. • Enter **window** *frames* to set the a polling window size in number of frames. The range is 1 to 65535; each value is a multiple of 10000 frames. The default is 1000.
Step 7	**ethernet oam link-monitor frame-seconds** {**threshold** {**high** {*high-seconds* | **none**} | **low** {*low-seconds*}} | **window** *milliseconds*}	(Optional) Configure frame-seconds high and low thresholds for triggering an error-frame-seconds link event. • Enter **threshold high** *high-seconds* to set a high threshold in number of seconds. The range is 1 to 900. You must enter a high threshold. • Enter **threshold high none** to disable the high threshold. • Enter **threshold low** *low-frames* to set a low threshold in number of frames. The range is 1 to 900. The default is 1. • Enter **window** *frames* to set the a polling window size in number of frames. The range is 100 to 9000; each value is a multiple of 100 milliseconds. The default is 1000.

	Command	Purpose
Step 8	**ethernet oam link-monitor high threshold action error-disable-interface**	(Optional) Configure the switch to put an interface in an error disabled state when a high threshold for an error is exceeded.
Step 9	**exit**	Return to global configuration mode.
Step 10	**interface** *interface-id*	Define an Ethernet OAM interface, and enter interface configuration mode.
Step 11	**source-template** *template-name*	Associate the template to apply the configured options to the interface.
Step 12	**end**	Return to privileged EXEC mode.
Step 13	**show ethernet oam status** [**interface** *interface-id*]	Verify the configuration.
Step 14	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of each command to remove the option from the template. Use the **no source-template** *template-name* to remove the source template association.

EXAMPLE

```
Switch(config)# template oam-temp
Switch(config-template)# ethernet oam link-monitor receive-crc window 99
Switch(config-template)# ethernet oam link-monitor symbol-period threshold high 299
Switch(config-template)# ethernet oam link-monitor frame window 399
Switch(config-template)# ethernet oam link-monitor frame-period threshold high 599
Switch(config-template)# ethernet oam link-monitor frame-seconds window 699
Switch(config-template)# ethernet oam link-monitor high threshold action
error-disable-interface
Switch(config-template)# exit
Switch(config)# interface gigabitEthernet 3/8
Switch(config-if)# source template oam-temp
Switch(config-if)# exit
Switch(config)# exit
```

Displaying Ethernet OAM Protocol Information

You can use the privileged EXEC commands in the following table to display Ethernet OAM protocol information.

Command	Purpose
show ethernet oam discovery [**interface** *interface-id*]	Displays discovery information for all Ethernet OAM interfaces or the specified interface.
show ethernet oam statistics [**interface** *interface-id*]	Displays detailed information about Ethernet OAM packets.
show ethernet oam status [**interface** *interface-id*]	Displays Ethernet OAM configuration for all interfaces or the specified interface.
show ethernet oam summary	Displays active Ethernet OAM sessions on the switch.

Enabling Ethernet Loopback

Service providers can use per-port and per VLAN Ethernet loopback to test connectivity at initial startup, to test throughput, and to test quality of service (QoS) in both directions. The switch supports two types of loopback:

- Facility loopback allows per-port or per-port, per-VLAN loopback of traffic. It provides an alternate method to Ethernet OAM remote loopback (see the "Enabling Ethernet OAM Remote Loopback" section on page 17-38) to test connectivity across multiple switches. You can exchange (swap) MAC destination and source addresses to allow a packet to cross multiple switches between the test head and a test switch.

  Per-port facility loopback puts the port into a loopback state where the link is up, but the line protocol is down for regular traffic. The switch loops back all received traffic.

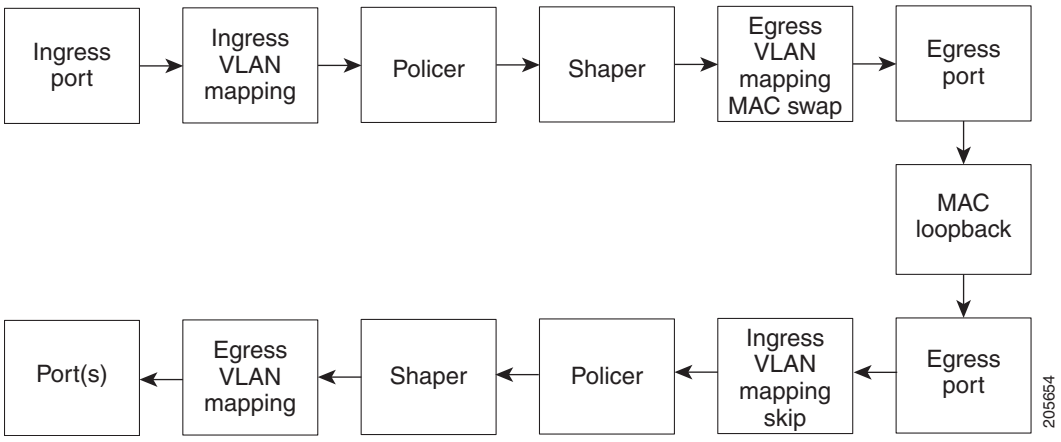
  When you configure per-port, per-VLAN loopback by entering the **vlan** *vlan-list* keywords, the other VLANs on the port continue to switch traffic normally, allowing nondisruptive loopback testing.

- Terminal loopback allows testing of full-path QoS in both directions. Terminal loopback puts the port into a state where it appears to be up but the link is actually down externally, and no packets are sent. Configuration changes on the port immediately affect the traffic being looped back.

  With terminal loopback, traffic that is looped back goes through the forwarding path a second time. If MAC swap is not configured. looped-back multicast or broadcast traffic is flooded on that VLAN. The packet then goes out the other ports twice, once from the ingress packet and once from the looped-back packet. See Figure 17-3.

  You can configure only one terminal loopback per switch.

Figure 17-3 Terminal Loopback Packet Flow



By default, no loopbacks are configured.

Ethernet loopback has these characteristics:

- You can configure Ethernet loopback only on physical ports, not on VLANs or port channels.
- You can configure one loopback per port and a maximum of two loopbacks per switch.
- You can configure only one terminal loopback per switch.
- The port ends the loopback after a port event, such as a shutdown or change from a switch port to a routed port.

- When you configure VLAN loopback by entering the **vlan** *vlan-list* keywords, the VLANs are tunneled into an internal VLAN that is not forwarded to any ports. The tunnel ends at the egress, so it is transparent to the user.
- VLAN loopback is not supported on nontrunk interfaces.
- Terminal loopback is not supported on routed interfaces.
- You cannot configure SPAN and loopback on the switch at the same time. If you try to configure SPAN on any port while loopback is configured, you receive an error message.
- If a port is a Flex Link port or belongs to an EtherChannel, it cannot be put into a loopback state. If loopback is active, you cannot add a port to a Flex Link or EtherChannel.
- Port loopback shares hardware resources with the VLAN mapping feature. If not enough TCAM resources are available because of VLAN-mapping configuration, when you attempt to configure loopback, you receive an error message, and the configuration is not allowed.

Configuring Ethernet Facility Loopback

BEFORE YOU BEGIN

Review the "Enabling Ethernet Loopback" section on page 17-47.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Define an interface, and enter interface configuration mode.
Step 3	**ethernet loopback facility** [**vlan** *vlan-list*] [**mac-address** {**swap** | **copy**}] [**timeout** {*seconds* | **none**}] **supported**	Configure Ethernet facility loopback on the interface. The keywords have these meanings: • (Optional) Enter **vlan** *vlan-list* to configure VLAN loopback for nondisruptive loopback testing. Other VLANs on the port continue to switch traffic. • (Optional) Enter **mac-address swap** to configure the switch to swap the MAC source and destination addresses for the loopback action. • (Optional) Enter **mac-address copy** to configure the switch to copy the MAC source and destination addresses for the loopback action. This is the default action if the **mac-address** option is not configured. • (Optional) Enter **timeout** *seconds* to set a loopback timeout period. The range is from 5 to 300 seconds. The default is 60 seconds. • (Optional) Enter **timeout none** to set the loopback to not time out.

	Command	Purpose
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**ethernet loopback** {**start** *interface-id* | **stop** {*interface-id* | **all**}	Turn on (**start**) Ethernet loopback on an interface, or turn off (**stop**) Ethernet loopback on an interface or on all interfaces. **Note** When you enter the command to start loopback, you receive a message that this is an intrusive loopback on the port or VLAN and that you will not be able to pass packets. You must confirm the command.
Step 6	**show ethernet loopback** [*interface-id*] **show interface** *interface-id*, **show interface status**, **show log**	Verify the configuration for the switch or for an interface. Verify that loopback is running (has been started) on an interface.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To stop an active loopback session on an interface or to stop all active loopback sessions, enter the **ethernet loopback stop** {*interface-id* | **all**} privileged EXEC command. To remove the Ethernet facility loopback configuration, enter the **no ethernet loopback** interface configuration command.

EXAMPLE

This example shows how to configure an Ethernet loopback to swap the MAC source and destination addresses. to never time out, and to start the loopback process. You must confirm the command before loopback starts.

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# ethernet loopback facility mac-address swap timeout none supported
Switch(config-if)# end
Switch# ethernet loopback start gigabitethernet 0/1
This is an intrusive loopback.
Therefore, while you test Ethernet connectivity,
you will be unable to pass traffic across that link.
Proceed with Local Loopback? [confirm]
```

This is the output from the **show ethernet loopback** privileged EXEC command for the previous configuration:

```
Switch# show ethernet loopback
====================================
Loopback Session 0  : Interface Gi0/1
Direction           : facility
Type                : port
Status              : configured
MAC Mode            : swap
Time out            : none.
```

Configuring Ethernet Terminal Loopback

BEFORE YOU BEGIN

Review the "Enabling Ethernet Loopback" section on page 17-47.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Define an interface, and enter interface configuration mode.
Step 3	**ethernet loopback terminal** [**mac-address** {**swap** | **copy**}] [**timeout** {*seconds* | **none**}] **supported**	Configure Ethernet terminal loopback to test QoS on the interface. The keywords have these meanings: • (Optional) Enter **mac-address swap** to configure the switch to swap the MAC source and destination addresses for the loopback action. • (Optional) Enter **mac-address copy** to configure the switch to copy the MAC source and destination addresses for the loopback action. This is the default action if the **mac-address** option is not configured. • (Optional) Enter **timeout** *seconds* to set a loopback timeout period. The range is from 5 to 300 seconds. The default is 60 seconds. • (Optional) Enter **timeout none** to set the loopback to not time out.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**ethernet loopback** {**start** | **stop**} {*interface-id*}	Turn on (**start**) or turn off (**stop**) Ethernet loopback on an interface. **Note** If you try to start terminal loopback on a routed interface, you receive an error message and you are not able to start the loopback.
Step 6	**show ethernet loopback** [*interface-id*] **show interface** *interface-id*, **show interface status**, **show log**	Verify the configuration for the switch or for an interface. Verify that loopback is running (has been started) on an interface.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable Ethernet terminal configuration, enter the **no ethernet loopback** interface configuration command.

EXAMPLE

This example shows how to configure an Ethernet terminal loopback to test QoS on the interface, to swap the MAC source and destination addresses, to time out after 30 seconds, and to start the loopback process:

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# ethernet loopback terminal mac-address swap timeout 30 supported
Switch(config-if)# end
Switch# ethernet loopback start gigabitethernet 0/1
```

Information About 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). E-LMI relies on the OAM Ethernet Infrastructure to interwork with CFM for end-to-end status of Ethernet virtual connections (EVCs) across CFM domains.

OAM manager, which streamlines interaction between any two OAM protocols, handles the interaction between CFM and E-LMI. This interaction is unidirectional, running only from OAM manager to E-LMI on the UPE side of the switch. Information is exchanged either as a result of a request from E-LMI or triggered by OAM when it received notification of a change from the OAM protocol. This type of information is relayed:

- EVC name and availability status
- Remote UNI name and status
- Remote UNI counts

You can configure Ethernet virtual connections (EVCs), service VLANs, UNI ids (for each CE-to-PE link), and UNI count and attributes. You need to configure CFM to notify the OAM manager of any change to the number of active UNIs and or the remote UNI ID for a given S-VLAN domain.

You can configure the switch as either the customer-edge device or the provider-edge device.

E-LMI Interaction with OAM Manager

No interactions are required between E-LMI and OAM manager on the CE side. On the UPE side, OAM manager defines an abstraction layer that relays data collected from OAM protocols (in this case CFM) running within the metro network to the E-LMI switch. The information flow is unidirectional (from OAM manager to the E-LMI) but is triggered in one of two ways:

- Synchronous data flow triggered by a request from the E-LMI
- Asynchronous data flow triggered by OAM manager when it receives notification from CFM that the number of remote UNIs has changed

This data includes:

- EVC name and availability status (active, not active, partially active, or not defined)
- Remote UNI name and status (up, disconnected, administratively down, excessive FCS failures, or not reachable)

- Remote UNI counts (the total number of expected UNIs and the actual number of active UNIs)

The asynchronous update is triggered only when the number of active UNIs has changed.

CFM Interaction with OAM Manager

When there is a change in the number of active UNIs or remote UNI ID for a given S-VLAN or domain, CFM asynchronously notifies the OAM manager. A change in the number of UNIs might (or might not) cause a change in EVC status. OAM manager calculates EVC status given the number of active UNIs and the total number of associated UNIs.

Note If crosscheck is disabled, no SNMP traps are sent when there is a change in the number of UNIs.

Configuring E-LMI

For E-LMI to work with CFM, you configure Ethernet virtual connections (EVCs), Ethernet service instances (EFPs), and E-LMI customer VLAN mapping. Most of the configuration occurs on the PE switch on the interfaces connected to the CE device. On the CE switch, you only need to enable E-LMI on the connecting interface. Note that you must configure some OAM parameters, for example, EVC definitions, on PE devices on both sides of a metro network.

This section includes the following topics:

Default E-LMI Configuration

Ethernet LMI is globally disabled by default. When enabled, the switch is in provider-edge (PE) mode by default.

When you globally enable E-LMI by entering the **ethernet lmi global** global configuration command, it is automatically enabled on all interfaces. You can also enable or disable E-LMI per interface to override the global configuration. The E-LMI command that is given last is the command that has precedence.

There are no EVCs, EFP service instances, or UNIs defined.

UNI bundling service is bundling with multiplexing.

E-LMI and OAM Manager Configuration Guidelines

OAM manager is an infrastructural element and requires two interworking OAM protocols, in this case CFM and E-LMI. For OAM to operate, the PE side of the connection must be running CFM and E-LMI.

- E-LMI is not supported on routed ports, EtherChannel port channels or ports that belong to an EtherChannel, private VLAN ports, or 802.1Q tunnel ports.
- You cannot configure E-LMI on VLAN interfaces.
- When you enable E-LMI globally or on an interface, the switch is in PE mode by default, You must enter the **ethernet lmi ce** global configuration command to enable the switch or interface in customer-edge mode.
- When the switch is configured as a CE device, the **service instance** and **ethernet uni** interface commands are visible but not supported.

Configuring the OAM Manager

Follow this procedure to configure OAM manager on a PE switch.

BEFORE YOU BEGIN

Review the "Information About E-LMI" section on page 17-51 and "E-LMI and OAM Manager Configuration Guidelines" section on page 17-52.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ethernet cfm domain** *domain-name* **level** *level-id*	Define a CFM domain, set the domain level, and enter ethernet-cfm configuration mode for the domain. The maintenance level number range is 0 to 7.
Step 3	**service** *csi-id* **vlan** *vlan-id*	Define a universally unique customer service instance (CSI) and VLAN ID within the maintenance domain. • *csi-id*—a string of no more than 100 characters that identifies the CSI. • *vlan-id*—VLAN range is from 1 to 4095. You cannot use the same VLAN ID for more than one domain at the same level.
Step 4	**exit**	Returns the CLI to Ethernet CFM configuration mode.
Step 5	**exit**	Return to global configuration mode.
Step 6	**ethernet evc** *evc-id*	Define an Ethernet virtual connection (evc), and enter evc configuration mode. The identifier can be up to 100 characters in length.

	Command	Purpose
Step 7	**oam protocol cfm svlan** *vlan-id* **domain** *domain-name*	Configure the EVC OAM protocol as CFM, and identify the service provider VLAN-ID (S-VLAN-ID) for the CFM domain maintenance level as configured in Steps 2 and 3. **Note** If the CFM domain does not exist, the command is rejected, and an error message appears.
Step 8	**uni count** *value*	(Optional) Set the UNI count for the EVC. The range is 2 to 1024; the default is 2. If the command is not entered, the service defaults to a point-to-point service. If you enter a value of 2, you have the option to select point-to-multipoint service. If you configure a value of 3 or greater, the service is point-to-multipoint. **Note** You should know the correct number of maintenance end points in the domain. If you enter a value greater than the actual number of end points, the UNI status will show as partially active even if all end points are up; if you enter a uni count less than the actual number of end points, status might show as active, even if all end points are not up.
Step 9	**exit**	Return to global configuration mode.
Step 10	Repeat Steps 2 to 5 for other CFM domains that you want OAM manager to monitor.	
Step 11	**interface** *interface-id*	Specify a physical interface connected to the CE device, and enter interface configuration mode.
Step 12	**service instance** *efp-identifier* **ethernet** [*evc-id*]	Configure an Ethernet service instance (EFP) on the interface, and enter ethernet service configuration mode. • The EFP identifier is a per-interface service identifier that does not map to a VLAN. The EFP identifier range is 1 to 4967295. • (Optional) Enter an *evc-id* to attach an EVC to the EFP.

	Command	Purpose
Step 13	**ethernet lmi ce-vlan map** {*vlan-id* | **any** | **default** | **untagged**}	Configure an E-LMI customer VLAN-to-EVC map for a particular UNI. The keywords have these meanings: • For **vlan** *vlan-id*, enter the customer VLAN ID or IDs to map to as single VLAN-ID (1 to 4094), a range of VLAN-IDs separated by a hyphen, or a series of VLAN IDs separated by commas. • Enter **any** to map all VLANs (untagged or 1 to 4094). • Enter **default** to map the default EFP. You can use **default** keyword only if you have already mapped the service instance to a VLAN or group of VLANs. • Enter **untagged** to map untagged VLANs.
Step 14	**exit**	Return to interface configuration mode.
Step 15	**ethernet uni id** *name*	Configure an Ethernet UNI ID. The name should be unique for all the UNIs that are part of a given customer service instance and can be up to 64 characters in length. When a UNI id is configured on a port, that ID is used as the default name for all MEPs configured on the port, unless a name is explicitly configured for a given MEP. **Note** This command is required on all ports that are directly connected to CE devices. If the specified ID is not unique on the device, an error message appears.
Step 16	**ethernet uni** {**bundle** [**all-to-one**] | **multiplex**}	(Optional) Set UNI bundling attributes: • If you enter **bundle** <cr>, the UNI supports bundling without multiplexing (only one EVC with one or multiple VLANs be mapped to it). • If you enter **bundle all-to-one**, the UNI supports a single EVC and all VLANs are mapped to that EVC. • If you enter **multiplex**, the UNI supports multiplexing without bundling (one or more EVCs with a single VLAN mapped to each EVC). If you do not configure bundling attributes, the default is bundling with multiplexing (one or more EVCs with one or more VLANs mapped to each EVC).
Step 17	**end**	Return to privileged EXEC mode.

	Command	Purpose
Step 18	**show ethernet service evc** {**detail** | **id** *evc-id* | **interface** *interface-id*}	Verify the configuration.
Step 19	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** forms of the commands to delete an EVC, EFP, or UNI ID, or to return to default configurations.

Note If you configure, change, or remove a UNI service type, EVC, EFP, or CE-VLAN configuration, all configurations are checked to make sure that the configurations match (UNI service type with EVC or EFP and CE-VLAN configuration). The configuration is rejected if the configurations do not match.

EXAMPLE

```
Switch(config)# ethernet cfm domain abc level 3
Switch(config-ecfm)# service test vlan 5
Switch(config-ecfm-srv)# exit
Switch(config-ecfm)# exit
Switch(config)# ethernet evc test1
Switch(config-evc)# oam protocol cfm svlan 5 domain abc
Switch(config-evc)# exit
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# service instance 10 ethernet test
Switch(config-if-srv)# ethernet lmi ce-vlan map 20
Switch(config-if-svc)# exit
Switch(config-if)# ethernet uni id test2
Switch(config-if)# end
```

Enabling E-LMI

You can enable E-LMI globally or on an interface and you can configure the switch as a PE or a CE device. Note that the order of the global and interface commands determines the configuration. The command that is entered last has precedence.

BEFORE YOU BEGIN

Review the "Information About E-LMI" section on page 17-51 and "E-LMI and OAM Manager Configuration Guidelines" section on page 17-52.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ethernet lmi global**	Globally enable E-LMI on all interfaces. By default, the switch is a PE device.
Step 3	**ethernet lmi ce**	(Optional) Configure the switch as an E-LMI CE device.

	Command	Purpose
Step 4	**interface** *interface-id*	Define an interface to configure as an E-LMI interface, and enter interface configuration mode.
Step 5	**ethernet lmi interface**	Configure Ethernet LMI on the interface. If E-LMI is enabled globally, it is enabled on all interfaces unless you disable it on specific interfaces. If E-LMI is disabled globally, you can use this command to enable it on specified interfaces.
Step 6	**ethernet lmi** {**n391** *value* | **n393** *value* | **t391** *value*| **t392** *value*}	Configure E-LMI parameters for the UNI. The keywords have these meanings: • **n391** *value*—Set the event counter on the customer equipment. The counter polls the status of the UNI and all Ethernet virtual connections (EVCs). The range is from 1 to 65000; the default is 360. • **n393** *value*—Set the event counter for the metro Ethernet network. The range is from 1 to 10; the default is 4. • **t391** *value*—Set the polling timer on the customer equipment. A polling timer sends status enquiries and when status messages are not received, records errors. The range is from 5 to 30 seconds; the default is 10 seconds. • **t392** *value*—Set the polling verification timer for the metro Ethernet network or the timer to verify received status inquiries. The range is from 5 to 30 seconds, or enter 0 to disable the timer. The default is 15 seconds. **Note** The **t392** keyword is not supported when the switch is in CE mode.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show ethernet lmi evc**	Verify the configuration.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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.

EXAMPLE

```
Switch(config)# ethernet lmi global
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ethernet lmi t391 30
Switch(config-if)# end
```

Ethernet OAM Manager Configuration Example

This is a simple example of configuring CFM and E-LMI with OAM manager on a PE device and on a CE device. You can configure the switch as either the PE device or the CE device.

Provider-Edge Device Configuration

This example shows a sample configuration of OAM manager, CFM, and E-LMI on the PE device:

```
Switch# config t
Switch(config)# ethernet cfm domain Top level 7
Switch(config)# ethernet cfm domain Provider level 4
Switch(config-ether-cfm)# service customer_1 vlan 101
Switch(config-ether-cfm)# mep crosscheck mpid 404 vlan 101
Switch(config-ether-cfm)# exit
Switch(config)# ethernet cfm domain Operator_level 2
Switch(config-ether-cfm)# service operator_1 vlan 101
Switch(config-ether-cfm)# exit
Switch(config)# ethernet cfm enable
Switch(config)# ethernet evc test1
Switch(config-evc)# oam protocol cfm svlan 101 domain Provider
Switch(config-evc)# exit
Switch(config)# ethernet evc 101
Switch(config-evc)# uni count 3
Switch(config-evc)# oam protocol cfm svlan 101 domain Operator
Switch(config-evc)# exit
Switch(config)# ethernet lmi global
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ethernet cfm mip level 7
Switch(config-if)# ethernet cfm mep level 4 mpid 200 vlan 200
Switch(config-if)# service instance 101 ethernet test1
Switch(config-if-srv)# ethernet lmi ce-vlan map 101
Switch(config-if-srv)# exit
Switch(config-if)# exit
Switch(config)# ethernet cfm cc enable level 2-4 vlan 101
Switch(config)# exit
```

Customer-Edge Device Configuration

This example shows the commands necessary to configure E-LMI on the CE device. The switch can be configured as the CE device. The example enables E-LMI globally, but you can also enable it only on a specific interface. However, if you do not enter the **ethernet lmi ce** global configuration command, the interface will be in PE mode by default.

```
Switch# config t
Switch(config)# ethernet lmi global
Switch(config)# ethernet lmi ce
Switch(config)# exit
```

Note For E-LMI to work, any VLANs used on the PE device must also be created on the CE device. Create a VLAN by entering the **vlan** *vlan-id* global configuration command on the CE device, where the *vlan-ids* match those on the PE device and configure these VLANs as allowed VLANs by entering the **switchport trunk allowed vlan** *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 and OAM Manager Information

Command	Purpose
show ethernet lmi evc [**detail** *evc-id* [**interface** *interface-id*] | **map interface** *type number*]	Displays details sent to the CE from the status request poll about the E-LMI EVC.
show ethernet lmi parameters interface *interface-id*	Displays Ethernet LMI interface parameters sent to the CE from the status request poll.
show ethernet lmi statistics interface *interface-id*	Displays Ethernet LMI interface statistics sent to the CE from the status request poll.
show ethernet lmi uni map interface [*interface-id*]	Displays information about the E-LMI UNI VLAN map sent to the CE from the status request poll.
show ethernet service evc {**detail** | **id** *evc-id* | **interface** *interface-id*}	Displays information about the specified Ethernet virtual connection (EVC) customer-service instance or all configured service instances.
show ethernet service instance {**detail** | **id** *efp-identifier* **interface** *interface-id* | **interface** *interface-id*}	Displays information relevant to the specified Ethernet service instances (EFPs).
show ethernet service interface [*interface-id*] [**detail**]	Displays information about OAM manager interfaces.

Ethernet CFM and Ethernet OAM Interaction

You can also configure the OAM Manager infrastructure for interaction between CFM and Ethernet OAM. When the Ethernet OAM Protocol is running on an interface that has CFM MEPs configured, Ethernet OAM informs CFM of the state of the interface. Interaction is unidirectional from the Ethernet OAM to the CFM Protocol, and the only information exchanged is the user network interface port status.

The Ethernet OAM Protocol notifies CFM when these conditions occur:

- Error thresholds are crossed at the local interface.

  CFM responds to the notification by sending a port status of *Local_Excessive_Errors* in the Port StatusType Length Value (TLV).

- Ethernet OAM receives an OAMPDU from the remote side showing that an error threshold is exceeded on the remote endpoint.

  CFM responds to the notification by sending a port status of *Remote_Excessive_Errors* in the Port Status TLV.

- The local port is set into loopback mode.

  CFM responds by sending a port status of Test in the Port Status TLV.

- The remote port is set into loopback mode.

  CFM responds by sending a port status of Test in the Port Status TLV.

This section includes the following topics:

- Configuring Ethernet OAM Interaction with CFM, page 17-60
- Ethernet OAM and CFM Configuration Example, page 17-62

For more information about CFM and interaction with Ethernet OAM, see the *Carrier Ethernet Configuration Guide, Cisco IOS Release 15M&T.*

Configuring Ethernet OAM Interaction with CFM

For Ethernet OAM to function with CFM, you must configure an Ethernet Virtual Circuit (EVC) and the OAM manager, and associate the EVC with CFM. You must use an up MEP for interaction with the OAM manager.

Note If you configure, change, or remove a UNI service type, EVC, Ethernet service instance, or CE-VLAN configuration, all configurations are verified to ensure that the UNI service types match the EVC configuration and that Ethernet service instances are matched with the CE-VLAN configuration. Configurations are rejected if the pairs do not match.

Configuring the OAM Manager

Follow this procedure to configure the OAM manager on a PE device.

BEFORE YOU BEGIN

Review the "Information About E-LMI" section on page 17-51 and "E-LMI and OAM Manager Configuration Guidelines" section on page 17-52.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ethernet cfm domain** *domain-name* **level** *level-id*	Define a CFM domain, set the domain level, and enter ethernet-cfm configuration mode for the domain. The maintenance level number range is 0 to 7.
Step 3	**service** *csi-id* **vlan** *vlan-id*	Define a universally unique customer service instance (CSI) and VLAN ID within the maintenance domain. • *csi-id*—String of no more than 100 characters that identifies the CSI. • *vlan-id*—VLAN range is from 1 to 4095. You cannot use the same VLAN ID for more than one domain at the same level.
Step 4	**exit**	Return to global configuration mode.
Step 5	**ethernet evc** *evc-id*	Define an EVC, and enter EVC configuration mode
Step 6	**oam protocol cfm svlan** *vlan-id* **domain** *domain-name*	Configure the EVC OAM protocol as CFM, and identify the service provider VLAN-ID (S-VLAN-ID) for the CFM domain maintenance level as configured in Steps 2 and 3.

	Command	Purpose
Step 7	**exit**	Return to global configuration mode.
Step 8	Repeat Steps 2 through 7 to define other CFM domains that you want OAM manager to monitor.	
Step 9	**ethernet cfm enable**	Globally enable CFM.
Step 10	**end**	Return to privileged EXEC mode.
Step 11	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

```
Switch(config)# ethernet cfm domain cstmr1 level 3
Switch(config-ether-cfm)# service csi2 vlan 10
Switch(config-ether-cfm)# exit
Switch(config)# ethernet evc 50
Switch(config-evc)# oam protocol cfm svlan 10 domain cstmr1
Switch(config-evc)# exit
Switch(config)# end
```

Enabling Ethernet OAM

BEFORE YOU BEGIN

Review the "Information About E-LMI" section on page 17-51 and "E-LMI and OAM Manager Configuration Guidelines" section on page 17-52.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Define an interface to configure as an Ethernet OAM interface and enter interface configuration mode.
Step 3	**ethernet oam** [**max-rate** *oampdus* | **min-rate** *seconds* | **mode** {**active** | **passive**} | **timeout** *seconds*]	Enable Ethernet OAM on the interface • (Optional) Enter **max-rate** *oampdus* to set the maximum rate (per second) to send OAM PDUs. The range is 1 to 10 PDUs per second; the default is 10. • (Optional) Enter **min-rate** *seconds* to set the minimum rate in seconds.The range is 1 to 10 seconds. • (Optional) Set the OAM client **mode** as **active** *or* **passive.** The default is **active.** • (Optional) Enter **timeout** *seconds* to set the time after which a device declares the OAM peer to be nonoperational and resets its state machine. The range is 2 to 30 seconds; the default is 5 seconds.

	Command	Purpose
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.

EXAMPLE

```
Switch(config)# interface ethernet 1/3
Switch(config-if)# ethernet oam max-rate 50
Switch(config-if)# end
```

Ethernet OAM and CFM Configuration Example

These are example configurations of the interworking between Ethernet OAM and CFM in a sample service provider network with a provider-edge switch connected to a customer edge switch at each endpoint. You must configure CFM, E-LMI, and Ethernet OAM between the customer edge and the provider edge switch.

Customer-edge switch 1 (CE1) configuration:

```
Switch# config t
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# port-type nni
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)# service instance 10 ethernet BLUE
Switch(config-if-srv)# ethernet lmi ce-vlan map 10
Switch(config-if-srv)# exit
```

Provider-edge switch 2 (PE2) configuration:

```
Switch# config t
Switch(config)# interface gigabitethernet1/20
Switch(config-if)# switchport mode trunk
Switch(config-if)# ethernet cfm mip level 7
Switch(config-if)# ethernet cfm mep level 4 mpid 101 vlan 10
Switch(config-if)# ethernet uni id 2004-20
Switch(config-if)# ethernet oam remote-loopback supported
Switch(config-if)# ethernet oam
Switch(config-if)# service instance 10 ethernet BLUE
Switch(config-if-srv)# ethernet lmi ce-vlan map 10
```

```
Switch(config-if-srv)# exit
```

Customer-edge switch 2 (CE2) configuration:

```
Switch# config t
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# port-type nni
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
Total Remote MEPs: 1
```

In addition, if you shut down the CE1 interface that connects to PE1, the remote PE2 port will show a PortState of *Down*.

Related Documents

- Carrier Ethernet Configuration Guide, Cisco IOS Release 15M&T
- Cisco IOS Carrier Ethernet Command Reference
- Cisco IOS IP SLAs Command Reference
- IP SLAs Configuration Guide, Cisco IOS Release 15M&T

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

Configuring Online Diagnostics

This chapter describes how to configure the online diagnostics on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*.

Note For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 18-9.

Information About 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 18-1 lists the diagnostic test IDs and names. For information about test attributes, see the output from the **show diagnostic content** privileged EXEC command.

Table 18-1 Diagnostic Tests

Test ID Number	Test Name
1	TestPortAsicStackPortLoopback
2	TestPortAsicLoopback
3	TestPortAsicCam
4	TestPortAsicRingLoopback
5	TestMicRingLoopback
6	TestPortAsicMem

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.
- Health-monitoring runs in the background.

Prerequisites

Before you enable any online diagnostics tests, enable console logging to see all warning messages. See Chapter 13, “Configuring System Message Logging.”

Guidelines and Limitations

- We recommend that when you are running disruptive tests that you only run the tests when connected through console. When disruptive tests are complete a warning message on the console recommends that you reload the system to return to normal operation: strictly follow this warning.
- While tests are running, all ports are shut down as a stress test is being performed with looping ports internally and external traffic might affect the test results. The switch must be rebooted to bring the switch to normal operation. When you issue the command to reload the switch, the system will ask you if the configuration should be saved. Do not save the configuration.
- If you are running the tests on other modules, after the test is initiated and complete, you must reset the module.
- After starting the tests, you cannot stop the testing process.

Default Settings

By default, health monitoring is disabled. When enabled, the switch generates a syslog message when a test fails.

Configuring Online Diagnostics

You must configure the failure threshold and the interval between tests before enabling diagnostic monitoring.

Scheduling Online Diagnostics

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 *Cisco IOS Configuration Fundamentals Command Reference, Release 15.2M&T*.

BEFORE YOU BEGIN

Review the "Information About Online Diagnostics" section on page 18-1 and "Guidelines and Limitations" section on page 18-2.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**diagnostic schedule test** {*name* | *test-id* | *test-id-range* | **all** | **basic** | **non-disruptive**} {**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 18-1. • *test-id*—ID number of the test that appears in the **show diagnostic content** command output. See Table 18-1. • *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. • **non-disruptive**—Nondisruptive health-monitoring 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.

	Command	Purpose
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** | **non-disruptive**} {**daily** *hh*:*mm* | **on** *mm dd yyyy hh*:*mm* | **weekly** *day-of-week hh*:*mm*} global configuration command to remove the scheduled tests.

EXAMPLE

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 2013 10:22
Switch(config)# end
Switch# show diagnostic schedule
Current Time = 10:21:24 UTC Thu Dec 4 2013

Diagnostic:

Schedule #1:
        To be run on December 4 2013 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
```

Configuring Health-Monitoring Diagnostics

You can configure health-monitoring diagnostic testing while a switch is connected to a live network. You can configure the execution interval for each health-monitoring test, enable the switch to generate a syslog message because of a test failure, and enable a specific test.

By default, health monitoring is disabled. When enabled, the switch generates a syslog message when a test fails.

BEFORE YOU BEGIN

Review the "Information About Online Diagnostics" section on page 18-1 and "Guidelines and Limitations" section on page 18-2.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**diagnostic monitor interval test** {*name* | *test-id* | *test-id-range* | **all**} *hh:mm:ss milliseconds day*	Configure the health-monitoring interval of the specified tests. Specify the tests by using one of these parameters: • *name*—Name of the test that appears in the **show diagnostic content** command output. See Table 18-1. • *test-id*—ID number of the test that appears in the **show diagnostic content** command output. See Table 18-1. • *test-id-range*—A range of test ID numbers separated by a hyphen or commas. • **all**—All of the diagnostic tests. When specifying the interval, set these parameters: • *hh:mm:ss*—Monitoring interval in hours, minutes, and seconds. The range for *hh* is 0 to 24, and the range for *mm* and *ss* is 0 to 60. • *milliseconds*—Monitoring interval in milliseconds (ms). The range is from 0 to 999. • *day*—Monitoring interval in number of days. The range is from 0 to 20.
Step 3	**diagnostic monitor syslog**	(Optional) Configure the switch to generate a syslog message when a health-monitoring test fails.
Step 4	**diagnostic monitor threshold test** {*name* | *test-id* | *test-id-range* | **all**} **failure count** *count*	(Optional) Set the failure threshold for the health-monitoring tests. Specify the tests by using one of these parameters: • *name*—Name of the test that appears in the **show diagnostic content** command output. See Table 18-1. • *test-id*—ID number of the test that appears in the **show diagnostic content** command output. See Table 18-1. • *test-id-range*—A range of test ID numbers separated by a hyphen or commas. • **all**—All of the diagnostic tests. The range for the failure threshold *count* is 0 to 99.

	Command	Purpose
Step 5	**diagnostic monitor test** {*name* | *test-id* | *test-id-range* | **all**}	Enable the specified health-monitoring tests. Specify the tests by using one of these parameters: • *name*—Name of the test that appears in the **show diagnostic content** command output. See Table 18-1. • *test-id*—ID number of the test that appears in the **show diagnostic content** command output. See Table 18-1. • *test-id-range*—ID numbers of the tests that appear in the **show diagnostic content** command output. • **all**—All of the diagnostic tests.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show diagnostic** {**content** | **post** | **result** | **schedule** | **status** | **switch**}	Display the online diagnostic test results and the supported test suites. See the "Displaying Online Diagnostic Tests and Results" section on page 18-8 for more information.
Step 8	**show running-config**	Verify your entries.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable diagnostic testing and return to the default settings, use these commands:

- To disable online diagnostic testing, use the **no diagnostic monitor test** {*name* | *test-id* | *test-id-range* | **all**} global configuration command.
- To return to the default health-monitoring interval, use the **no diagnostic monitor interval test** {*name* | *test-id* | *test-id-range* | **all**} global configuration command.
- To configure the switch to not generate a syslog message when the health-monitoring test fails, use the **no diagnostic monitor syslog** global configuration command.
- To return to the default failure threshold, use the **no diagnostic monitor threshold test** {*name* | *test-id* | *test-id-range* | **all**} **failure count** *count* global configuration command.

EXAMPLE

This example shows how to configure a health-monitoring test:

```
Switch(config)# diagnostic monitor threshold test 1 failure count 50
Switch(config)# diagnostic monitor interval test TestPortAsicRingLoopback
```

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

Note After starting the tests, you cannot stop the testing process.

BEFORE YOU BEGIN

- Configure the diagnostics tests as described in the "Configuring Online Diagnostics" procedure on page 18-3.
- Review the "Guidelines and Limitations" section on page 18-2.

DETAILED STEPS

Command	Purpose
diagnostic start test {*name* | *test-id* | *test-id-range* | **all** | **basic** | **non-disruptive**}	Start the diagnostic tests. Specify the tests by using one of these parameters: • *name*—Enter the name of the test. Use the **show diagnostic content** privileged EXEC command to display the test ID list. See Table 18-1. • *test-id*—Enter the ID number of the test. Use the **show diagnostic content** privileged EXEC command to display the test ID list. See Table 18-1. • *test-id-range*—Enter the range of test IDs by using integers separated by a comma and a hyphen. For more information, see the **diagnostic start** command in the *Cisco IOS Configuration Fundamentals Command Reference, Release 15.2M&T*. • **all**—Use this keyword when you want to run all of the tests. • **basic**—Use this keyword when you want to run the basic test suite. • **non-disruptive**—Use this keyword when you want to run the nondisruptive test suite.

EXAMPLE

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 a non-disruptive diagnostic test:

```
Switch# diagnostic start test non-disruptive
Switch#
*Mar  3 19:34:02.680: %DIAG-6-TEST_RUNNING: : Running TestPortAsicStackPortLoopback{ID=1}
..
*Mar  3 19:34:03.687: %DIAG-6-TEST_OK: : TestPortAsicStackPortLoopback{ID=1} has completed
successfully
```

This example shows how to start all of the basic diagnostic tests:

```
Switch# diagnostic start test all
```

Displaying Online Diagnostic Tests and Results

Command	Purpose
show diagnostic content	Displays the online diagnostics configured for a switch.
show diagnostic status	Displays the running diagnostic tests.
show diagnostic result [**detail** | **test** {*name* | *test-id* | *test-id-range* | **all** [**detail**]}]	Displays the specified online diagnostics test results.
show diagnostic switch [**detail**]	Displays the online diagnostics test results.
show diagnostic schedule	Displays the online diagnostics test schedule.
show diagnostic post	Displays the POST results. (The output is the same as the **show post** command output.)

EXAMPLE

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
---------

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 Tests : Begin
POST: Thermal 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
```

For more examples of other **show diagnostic** command outputs, see the "Examples" section of the **show diagnostic** command in the *Cisco IOS Configuration Fundamentals Command Reference, Release 15.2M&T*.

Configuration Example

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 2013 10:22
Switch(config)# end
Switch# show diagnostic schedule
Current Time = 10:21:24 UTC Thu Dec 4 2013

Diagnostic:

Schedule #1:
        To be run on December 4 2013 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
```

This example shows how to configure a health-monitoring test:

```
Switch(config)# diagnostic monitor threshold test 1 failure count 50
Switch(config)# diagnostic monitor interval test TestPortAsicRingLoopback
```

Related Documents

- Cisco IOS Master Command List, All Releases
- Cisco IOS Configuration Fundamentals Command Reference, Release 15.2M&T

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

Supported MIBs

This appendix lists the supported management information bases (MIBs) for this release on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*. This appendix includes the following sections:

MIB List

- BRIDGE-MIB (RFC1493)

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-AUTH-FRAMEWORK-MIB
- CISCO-CABLE-DIAG-MIB
- CISCO-CDP-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-DHCP-SNOOPING-MIB
- CISCO-ENTITY-ALARM-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENTITY-SENSOR MIB
- CISCO-ENTITY-VENDORTYPE-OID-MIB
- CISCO-ENVMON-MIB
- CISCO-EPM-NOTIFICATION-MIB
- CISCO-ERR-DISABLE-MIB
- CISCO-ETHER-CFM-MIB
- CISCO-ETHERNET-ACCESS-MIB

- CISCO-FLASH-MIB (Flash memory on all switches is modeled as removable flash memory.)
- CISCO-FTP-CLIENT-MIB
- CISCO-HSRP-MIB

Note Layer 3 MIBs are available only when the IP Services image is running on the switch.

- CISCO-HSRP-EXT-MIB (partial support)
- CISCO-IGMP-FILTER-MIB
- CISCO-IMAGE-MIB
- CISCO-IPSLA-ETHERNET-MIB

Note Available only when the IP Services image is running on the switch.

- CISCO-L2L3-INTERFACE-CONFIG-MIB
- CISCO-LAG-MIB
- CISCO-MAC-NOTIFICATION-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-NAC-NAD-MIB
- CISCO-PAE-MIB
- CISCO-PAGP-MIB
- CISCO-PING-MIB
- CISCO-POE-PD-MIB
- CISCO-PORT-QOS-MIB (the cportQosStats Table returns the values from the octets and packet counters, depending on switch configuration)
- CISCO-PRODUCTS-MIB
- CISCO-PROCESS-MIB
- CISCO-RTTMON-MIB
- CISCO-SMI-MIB
- CISCO-STACKMAKER-MIB
- CISCO-STP-EXTENSIONS-MIB
- CISCO-SYSLOG-MIB
- CISCO-TC-MIB
- CISCO-TCP-MIB
- CISCO-UDLDP-MIB
- CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB
- CISCO-VLAN-MEMBERSHIP-MIB
- CISCO-VTP-MIB
- ENTITY-MIB
- ETHERLIKE-MIB

- IDENTITY-MIB
- IEEE8021-PAE-MIB
- IEEE8023-LAG-MIB
- IF-MIB (In and out counters for VLANs are not supported.)
- IGMP-MIB
- INET-ADDRESS-MIB
- IPMROUTE-MIB
- LLDP MIB
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-FLASH-MIB
- OLD-CISCO-INTERFACES-MIB
- OLD-CISCO-IP-MIB
- OLD-CISCO-SYS-MIB
- OLD-CISCO-TCP-MIB
- OLD-CISCO-TS-MIB
- PIM-MIB
- RFC1213-MIB (Functionality is as per the agent capabilities specified in the CISCO-RFC1213-CAPABILITY.my.)
- RFC1253-MIB (OSPF-MIB)
- RMON-MIB
- RMON2-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-MPD-MIB
- SNMP-NOTIFICATION-MIB
- SNMP-TARGET-MIB
- SNMPv2-MIB
- TCP-MIB
- UDP-MIB

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.