Cisco Connected Grid Ethernet Switch Module Software Interface Card Configuration Guide

First Published: May 2012
Last Updated: February 2016

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 chapter provides an overview of the Cisco Connected Grid10-Port Ethernet Switch Module Interface Card (also known as a switch module or the CGR 2010 ESM). This chapter contains the following topics:

Note In this document, *IP* refers to IP Version 4 (IPv4) unless otherwise specified as IPv6.

Introduction

The CGR 2010 ESM is designed for internetworking in the energy industry, typically in power substations for substation automation and integration, as well as harsh environments such as electric substation environments, intelligent transportation trackside substations, downstream oil and gas, and other Connected Energy applications.

The CGR 2010 ESM is a double-wide switch module that is installed into the Cisco CGR 2010 router chassis. There are two models for this switch module:

Table 1-1 CGR 2010 ESM Copper Model

Model	Description
GRWIC-D-ES-2S-8PC (Copper model)	8x 10/100 Fast Ethernet ports, 1x dual-purpose port (10/100/1000 Base-T copper RJ-45 and 100/1000 SFP fiber), 1x 100/1000 SFP fiber-only port

Figure 1-1 GRWIC-D-ES-2S-8PC (Copper Model)

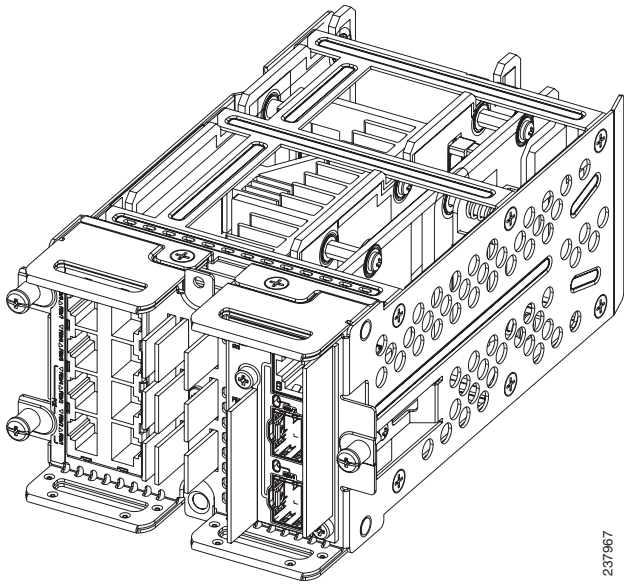
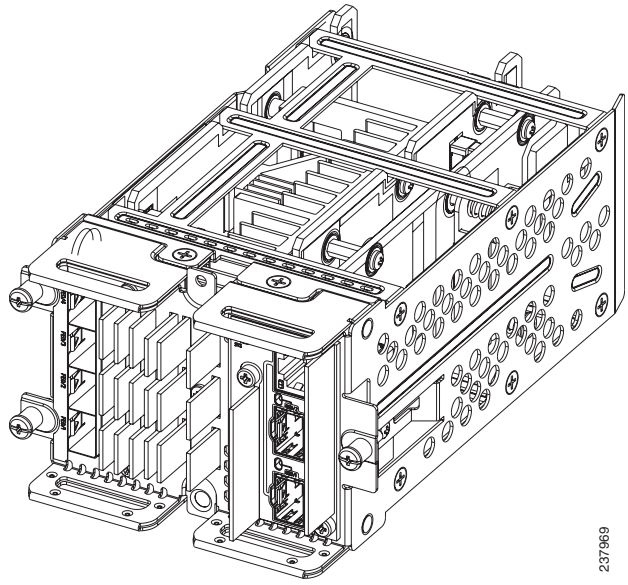


Table 1-2 CGR 2010 ESM SFP Fiber Model

Model	Description
GRWIC-D-ES-6S (SFP Fiber model)	4x 100BASE-FX SFP-module ports, 1x dual-purpose port (1x 10/100/1000Base-T copper RJ-45 port and 1x 100/1000 SFP fiber module port), 1x 100/1000 SFP fiber module port

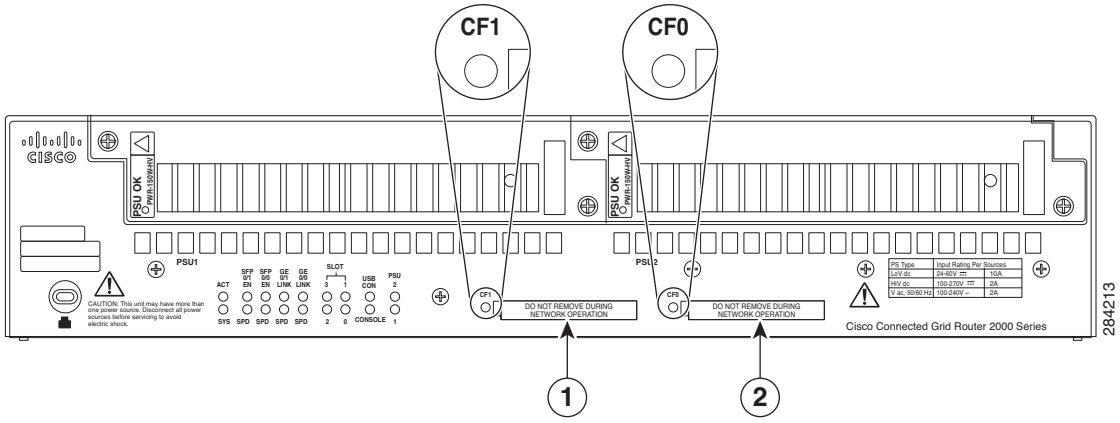
Figure 1-2 GRWIC-D-ES-6S (SFP Fiber Model)



Router Compact Flash Memory Cards

The router supports a maximum of two compact flash memory cards. The router ships with one compact flash card installed and supports a second, optional flash card that you can order with the router or supply separately. Figure 1-3 illustrates the location of the compact flash card slots on the router.

Figure 1-3 Cisco Connected Grid 2010 Router—Compact Flash Memory Card Slot Locations



Item	Label on Router	Description	Cisco IOS Interface Name
1	CF1	This slot supports an optional compact flash card that you can order with the router or supply separately. The Connected Grid Swap Drive feature is not supported on this slot.	**flash1:**
2	CF0	This is the required slot for use with the Connected Grid Swap Drive feature. The router comes with a compact flash card already installed in this slot. The Connected Grid Swap Drive feature is supported on this CF slot only.	**flash** or **flash0**:

For additional information about the router compact flash memory support, refer to the router hardware installation guide at:

http://www.cisco.com/en/US/products/ps10977/prod_installation_guides_list.html

Detecting and Validating the Switch Module

When you install the CGR 2010 ESM into the double-wide slot on the Cisco CGR 2010 router, the router identifies and validates the switch module.

Communication Between the Host Router and the Switch Module

The backplane interface on the CGR 2010 ESM is called *PortChannel48*. The backplane interface on the host router side is called **GigabitEthernet0/x/0** (interface **GigabitEthernet0/0/0** and/or interface **GigabitEthernet0/2/0**). The backplane interface provides communication between the host router and the switch module.

If the switch module is installed in slot0 of the CGR 2010 router, the interface **GigabitEthernet0/0/0** is created automatically. GigabitEthernet0/0/0 is the backplane interface connected to the switch module in slot0. This interface supports creation of subinterfaces for inter-VLAN routing functionality.

The PortChannel48 interface consists of eight 10/100 FastEthernet physical links that are grouped together to create a FastEtherChannel. For details, see Chapter 9, "EtherChannel Configuration Between the Switch Module and the Host Router."

Removing the Switch Module

Online Insertion and Removal (OIR) of the CGR 2010 ESM is not supported. For information on the correct procedure for removing the switch module from the router, see "Removing the Switch Module" in the *Cisco Connected Grid 10-Port Ethernet Switch Module Interface Card Getting Started Guide*.

Caution The Cisco CGR 2010 router does not support removing switch modules when the chassis is powered on. Removing the switch module when the router is running can result in undesirable behavior, such as resetting or damaging to the router.

About Router Reset and the Switch Module

The CGR 2010 ESM is a GRWIC (Grid Router WAN Interface Card) inserted into the Cisco CGR 2010 router. When the router crashes or the router is reloaded gracefully, the switch module remains up and running. In this state, the backplane interface is down, but the switch module can still occur between the front panel ports.

When the router starts to load the image (either through the manual or autoboot process), the router resets the switch module.

Caution Any unsaved configurations on the switch module will be lost if the CGR 2010 router is reloaded. Make sure you write the configurations to NVRAM on the switch module using the **write memory** command.

Switch Module Software Images and Interface Types

The CGR 2010 ESM ships with one of these software images installed:

- **CGR 2010 LAN base image:** This 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.

- **CGR 2010 IP services image:** In addition to features supported in the LAN based image, this 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).

The swtich has three different types of interfaces:

- Network Node Interfaces (NNIs)—connects to the service provider network
- User Network Interfaces (UNIs)—connects to customer networks
- 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).

Note By default, on startup, all ports on the switch module are enabled as NNIs. The default status for an NNI is administratively up to allow a service provider remote access to the switch module during initial configuration.

Switch Module Features

This section describes the following features:

- Performance Features, page 1-5
- Management Options, page 1-6
- Manageability Features, page 1-7

Performance Features

The CGR 2010 ESM provides the following performance features:

- Autosensing of port speed and auto negotiation of duplex mode on all switch module ports for optimizing bandwidth
- Automatic-medium dependent interface crossover (auto-MDIX) capability on 10/100 and 10/100/1000 Mbps interfaces that enable the interface to automatically detect the required cable connection type (straight-through or crossover), and to configure the connection appropriately.
- Support for routed frames up to 1998 bytes, for frames up to 9000 bytes that are bridged in hardware, and for frames up to 2000 bytes that are bridged by software
- IEEE 802.3x flow control on all ports (the switch module does not send pause frames)
- EtherChannel for enhanced fault tolerance and for providing up to 800 Mbps (Fast EtherChannel) full duplex of bandwidth between the switch modules, routers, and servers
- Forwarding of Layer 2 and Layer 3 packets at Gigabit line rate
- Per-port storm control for preventing broadcast, multicast, and unicast storms
- Port blocking on forwarding unknown Layer 2 unknown unicast, multicast, and bridged broadcast traffic
- Internet Group Management Protocol (IGMP) snooping for IGMP versions 1, 2, and 3 for efficiently forwarding multimedia and multicast traffic

- IGMP report suppression for sending only one IGMP report per multicast router query to the multicast devices (supported only for IGMPv1 or IGMPv2 queries)
- IGMP snooping querier support to configure the switch module to generate periodic IGMP General Query messages
- IGMP Helper to allow the switch module to forward a host request to join a multicast stream to a specific IP destination address (requires the IP services image)
- IGMP filtering for controlling the set of multicast groups to which hosts on a switch module port can belong
- IGMP throttling for configuring the action when the maximum number of entries is in the IGMP forwarding table
- IGMP configurable leave timer to configure the network's leave latency
- Multicast VLAN registration (MVR) to continuously send multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons with support for 512 multicast entries on a switch module
- MVR over trunk port (MVRoT) support to allow you to configure a trunk port as an MVR receiver port
- Multicast VLAN Registration (MVR) enhancements include the ability to configure 2000 MVR groups when the switch module is in dynamic MVR mode and a command (**mvr ringmode flood**) to ensure that forwarding in a ring topology is limited to member ports
- Switch Database Management (SDM) templates for allocating system resources to maximize support for user-selected features, including the dual-ipv4-and-ipv6 template for supporting IPv6 addresses
- RADIUS server load balancing to allow access and authentication requests to be distributed evenly across a server group

Management Options

The CGR 2010 ESM provides the following management features:

- **Command Line Interface** (CLI)—Cisco IOS software supports desktop-switching and multilayer-switching features

  Before you can access the switch module CLI, you must connect to the Cisco CGR 2010 router through the router console or through Telnet. Once you are connected to the Cisco CGR 2010 router, you must configure an IP address on the backplane Gigabit Ethernet interface connected to the switch module.

  To connect to the router, open a session to the switch module using the **service-module gigabitethernet** *0/x/0* **session** command in privileged EXEC mode on the router.

  For detailed information about using this CLI, see Chapter 3, "Access the Switch Module from the Host Router."
- **Cisco Configuration Engine**—Network management device that works with embedded Cisco IOS CNS Agents in the switch module software. You can automate initial configurations and configuration updates by generating switch module-specific configuration changes, sending them to the switch module, executing the configuration change, and logging the results. For more information about using Cisco IOS agents, see Chapter 5, "Cisco IOS Configuration Engine."

- **Cisco Configuration Professional**—GUI-based device management tool for Cisco access routers. It simplifies router, firewall, IPS, VPN, unified communications, WAN, and basic LAN configuration through easy-to-use wizards.
- **SNMP**—Includes SNMP management applications such as CiscoWorks2000 LAN Management Suite (LMS) and HP OpenView. You can manage from an SNMP-compatible management station that is running platforms such as HP OpenView or SunNet Manager. The switch module supports a comprehensive set of MIB extensions, and four remote monitoring (RMON) groups. For more information about using SNMP, see Chapter 14, "Quality of Service Configuration."

Manageability Features

The CGR 2010 ESM provides the following manageability features:

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

- MODBUS TCP support to connect to devices such as Intelligent Electronic Devices (IEDs), distributed controllers, substation routers, Cisco IP Phones, Cisco Wireless Access Points, and other network devices (such as redundant substation switches modules).
- Support for classification and prioritization of Generic Object-Oriented Substation Events (GOOSE) messages and SCADA messages, using QoS functionality
- Cisco-default Smart port macros for creating custom switch module configurations for simplified deployment across the network
- Express Setup for quickly configuring a switch module for the first time with basic IP information, contact information, switch module and Telnet passwords, and Simple Network Management Protocol (SNMP) information through a browser-based program. For more information about Express Setup, see "Running Express Setup" in the *Cisco Connected Grid 10-Port Ethernet Switch Module Interface Card Getting Started Guide*.
- Support for DHCP for configuration of switch module information (such as IP address, default gateway, hostname, and Domain Name System [DNS] and TFTP server names)
- DHCP relay for forwarding User Datagram Protocol (UDP) broadcasts, including IP address requests, from DHCP clients
- DHCP server for automatic assignment of IP addresses and other DHCP options to IP hosts
- DHCP-based auto-configuration and image update to download a specified configuration a new image to a large number of switch modules
- DHCP server port-based address allocation for the preassignment of an IP address to a switch module port
- Directed unicast requests to a DNS server for identifying a switch module through its IP address and its corresponding hostname, and to a TFTP server for administering software upgrades from a TFTP server
- Address Resolution Protocol (ARP) for identifying a switch module through its IP address and its corresponding MAC address
- Unicast MAC address filtering to drop packets with specific source or destination MAC addresses
- Configurable MAC address scaling that allows disabling MAC address learning on a VLAN to limit the size of the MAC address table

- Cisco Discovery Protocol (CDP) Versions 1 and 2 for network topology discovery and mapping between the switch module and other Cisco devices on the network (supported on NNIs by default, can be enabled on ENIs, but not supported on UNIs)
- Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED) for interoperability with third-party IP phones (supported only on NNIs or ENIs)
- Support for the LLDP-MED location TLV that provides location information from the switch module to the endpoint device
- Network Time Protocol (NTP) for providing a consistent timestamp to all switch modules from an external source
- Cisco IOS File System (IFS) for providing a single interface to all file systems that the switch module uses
- In-band management access for up to 16 simultaneous Telnet connections for multiple CLI-based sessions over the network
- In-band management access for up to five simultaneous, encrypted Secure Shell (SSH) connections for multiple CLI-based sessions over the network (requires the cryptographic versions of the switch module software)
- In-band management access through SNMP Versions 1, 2c, and 3 get and set requests
- Out-of-band management access through the Cisco CGR 2010 router console port to a directly attached terminal, or to a remote terminal through a serial connection or a modem
- Support for metro Ethernet operation, administration, and maintenance (OAM) IEEE 802.1ag Connectivity Fault Management (CFM), Ethernet Line Management Interface (E-LMI) on customer-edge and provider-edge switch modules, and 802.3ah Ethernet OAM discovery, link monitoring, remote fault detection, and remote loopback, and 802.3ah Ethernet OAM discovery, link monitoring, remote fault detection, and remote loopback
- Support for Ethernet loopback facility for testing connectivity to a remote device including VLAN loopback for non-disruptive loopback testing, and terminal loopback to test full-path QoS in both directions (requires the IP services image)
- Configuration replacement and rollback to replace the running configuration on a switch module with any saved Cisco IOS configuration file
- Source Specific Multicast (SSM) mapping for multicast applications to provide a mapping of source to allow IGMPv2 clients to utilize SSM, and allow listeners to connect to multicast sources dynamically and reduce dependencies on the application
- HTTP client can send requests to both IPv4 and IPv6 HTTP servers, and the HTTP server in Cisco IOS can service HTTP requests from both IPv4 and IPv6 HTTP clients (requires the IP services image)
- IPv6 supports stateless auto-configuration to manage link, subnet, and site addressing changes, such as management of host and mobile IP addresses (requires the IP services image)
- IPv6 supports stateless auto-configuration to manage link, subnet, and site addressing changes, such as management of host and mobile IP addresses (requires the IP services image)
- CPU utilization threshold trap monitors CPU utilization
- Support for including a hostname in the option 12 field of DHCPDISCOVER packets, providing identical configuration files to be sent by using the DHCP protocol
- DHCP Snooping enhancement to support the selection of a fixed string-based format for the circuit-id sub-option of the Option 82 DHCP field

Availability Features

The CGR 2010 ESM provides the following availability features:

- UniDirectional Link Detection (UDLD) and aggressive UDLD for detecting and disabling unidirectional links on fiber-optic interfaces caused by incorrect fiber-optic wiring or port faults
- 802.1D Spanning Tree Protocol (STP) for redundant backbone connections and loop-free networks (supported by default on NNIs, can be enabled on ENIs, not supported on UNIs). STP has these features:
  - Up to 128 supported spanning-tree instances
  - Per-VLAN spanning-tree plus (PVST+) for balancing load across VLANs
  - Rapid PVST+ for balancing load across VLANs and providing rapid convergence of spanning-tree instances
- 802.1s Multiple Spanning Tree Protocol (MSTP) on NNIs or ENIs for grouping VLANs into a spanning-tree instance, providing multiple forwarding paths for data traffic and load balancing, and providing rapid per-VLAN Spanning-Tree plus (rapid-PVST+) based on the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for rapid convergence of the spanning tree (by immediately transitioning root and designated port NNIs or spanning-tree enabled ENIs to the forwarding state)
- Optional spanning-tree features available in PVST+, rapid-PVST+, and MSTP modes on NNIs and ENIs, where spanning tree has been enabled:
  - Port Fast for eliminating the forwarding delay by enabling a spanning-tree port to immediately transition from the blocking state to the forwarding state
  - Bridge protocol data unit (BPDU) guard for shutting down Port Fast-enabled ports that receive BPDUs
  - BPDU filtering for preventing a Port Fast-enabled ports from sending or receiving BPDUs
  - Root guard for preventing switch modules outside the network core from becoming the spanning-tree root
  - Loop guard for preventing alternate or root port NNIs or ENIs from becoming designated ports because of a failure that leads to a unidirectional link
- Flex Link Layer 2 interfaces to backup one another as an alternative to STP for basic link redundancy in a nonloop network with pre-emptive switchover and bidirectional fast convergence; also referred to as the MAC address-table move update feature
- Flex Link Multicast Fast Convergence to reduce the multicast traffic convergence time after a Flex Link failure
- Link-state tracking to mirror the state of the ports that carry upstream traffic from connected hosts and servers, and to allow the failover of the server traffic to an operational link on another CGR 2010 ESM
- Support for Resilient Ethernet Protocol (REP) for improved convergence times and network loop prevention without the use of spanning tree
- Counter and timer enhancements to REP support
- Support for REP edge ports when the neighbor port is not REP-capable
- HSRP for Layer 3 router redundancy (requires IP services image)
- Equal-cost routing for link-level and switch module-level redundancy (requires IP services image)
- Shorter Resilient Ethernet Protocol (REP) hello: Changes the range of the REP link status layer (LSL) age timer from 3000 to 10000 ms in 500-ms intervals to 120 to 10000 ms in 40-ms intervals

VLAN Features

The CGR 2010 ESM provides the following VLAN features:

- Support for up to 1005 VLANs for assigning users to VLANs associated with appropriate network resources, traffic patterns, and bandwidth
- Support for VLAN IDs in the full 1 to 4094 range allowed by the 802.1Q standard
- VLAN Query Protocol (VQP) for dynamic VLAN membership
- 802.1Q trunking encapsulation on all ports for network moves, adds, and changes; management and control of broadcast and multicast traffic; and network security by establishing VLAN groups for high-security users and network resources
- VLAN 1 minimization for reducing the risk of spanning-tree loops or storms by allowing VLAN 1 to be disabled on any individual VLAN trunk link. With this feature enabled, no user traffic is sent or received on the trunk. The switch module CPU continues to send and receive control protocol frames.
- UNI-ENI isolated VLANs to isolate customer VLANs from VLANs of other customers on the same switch. Local switching does not occur among UNIs or ENIs on the switch module that belongs to the same UNI-ENI isolated VLAN.
- Private VLANs to address VLAN scalability problems, to provide a more controlled IP address allocation, and to allow Layer 2 ports to be isolated from ports on other switch modules
- Port security on a PVLAN host to limit the number of MAC addresses learned on a port, or define which MAC addresses may be learned on a port
- VLAN Flex Link Load Balancing to provide Layer 2 redundancy without requiring Spanning Tree Protocol (STP). A pair of interfaces configured as primary and backup links can load balance traffic based on VLAN.

Security Features

Note The CGR 2010 ESM provides security for the subscriber, the switch module, and the network.

The CGR 2010 ESM provides the security features, as described below.

Subscriber Security

- By default, local the switch module is disabled among subscriber ports to ensure that subscribers are isolated
- DHCP snooping to filter untrusted DHCP messages between untrusted hosts and DHCP servers
- DHCP Snooping Statistics **show** and **clear** commands to display and remove DHCP snooping statistics in summary or detail form
- IP source guard to restrict traffic on nonrouted interfaces by filtering traffic based on the DHCP snooping database and IP source bindings
- Dynamic ARP inspection to prevent malicious attacks on the switch module by not relaying invalid ARP requests and responses to other ports in the same VLAN

Switch Module Security

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

- Password-protected access (read-only and read-write access) to management interfaces for protection against unauthorized configuration changes
- Configuration file security so that only authenticated and authorized users have access to the configuration file, preventing users from accessing the configuration file by using the password recovery process
- Multi-level security for a choice of security level, notification, and resulting actions
- Port security option for limiting and identifying MAC addresses of the stations allowed to access the port
- Port security aging to set the aging time for secure addresses on a port
- LLDP (Link Layer Discovery Protocol) and LLLDP-MED (Media Extensions)—Adds support for 802.1AB link layer discovery protocol for interoperability in multi-vendor networks. Switches exchange speed, duplex, and power settings with end devices such as IP phones.
- UNI and ENI default port state is disabled
- Automatic control-plane protection to protect the CPU from accidental or malicious overload due to Layer 2 control traffic on UNIs or ENIs
- Configurable control plane security that provides service providers with the flexibility to drop customers control-plane traffic on a per-port, per-protocol basis. Allows configuring of ENI protocol control packets for CDP, STP, LLDP, and LACP.
- TACACS+, a proprietary feature for managing network security through a TACACS server
- RADIUS for verifying the identity of, granting access to, and tracking the actions of remote users through Authentication, Authorization and Accounting (AAA) services
- Kerberos security system to authenticate requests for network resources by using a trusted third-party (requires the cryptographic version of the switch module software)

Network Security

- Static MAC addressing for ensuring security
- Standard and extended IP Access Control Lists (ACLs) for defining security policies in both directions on routed interfaces (router ACLs) and VLANs and inbound on Layer 2 interfaces (port ACLs)
- IPv6 ACLs to be applied to interfaces to filter IPv6 traffic
- Extended MAC access control lists for defining security policies in the inbound direction on Layer 2 interfaces
- VLAN ACLs (VLAN maps) for providing intra-VLAN security by filtering traffic based on information in the MAC, IP, and TCP/UDP headers
- Source and destination MAC-based ACLs for filtering non-IP traffic
- 802.1x port-based authentication to prevent unauthorized devices (clients) from gaining access to the network, including the following features:

  - VLAN assignment for restricting 802.1x-authenticated users to a specified VLAN
  - Port security for controlling access to 802.1x ports
  - 802.1x accounting to track network usage
  - 802.1x readiness check to determine the readiness of connected end hosts before configuring 802.1x on the switch module
  - Network Edge Access Topology (NEAT) with 802.1x switch module supplicant, host authorization with Client Information Signalling Protocol (CISP), and auto-enablement to authenticate a switch module outside a wiring closet as a supplicant to another switch module
- Support for IP source guard on static hosts
- 802.1x User Distribution to allow deployments with multiple VLANs (for a group of users) to improve scalability of the network by load balancing users across different VLANs. Authorized users are assigned to the least populated VLAN in the group, assigned by RADIUS server.
- Support for 3DES and AES with version 3 of the Simple Network Management Protocol (SNMPv3). This release adds support for the 168-bit Triple Data Encryption Standard (3DES) and the 128-bit, 192-bit, and 256-bit Advanced Encryption Standard (AES) encryption algorithms to SNMPv3.
- Additional IPv6 support to include IPv6 eBGP, IPv6 SNMP, Syslog, and HTTP as well as IPv6 MLD snooping

QoS and CoS Features

The CGR 2010 ESM provides the following Quality of Service (QoS) and Class of Service (CoS) features:

- QoS features for implementing high-priority (low-latency) traffic via backplane between the switch module and the host CGR 2010 router. S*ee "Implementing High-Priority Traffic to the Host Router" section on page 14-95*. For more information, see also Chapter 9, "EtherChannel Configuration Between the Switch Module and the Host Router."
- Configurable control-plane queue assignment to assign control plane traffic for CPU-generated traffic to a specific egress queue
- Cisco Modular QoS Command-line (MQC) implementation
- Classification based on IP precedence, Differentiated Services Code Point (DSCP), and 802.1p CoS packet fields, ACL lookup, or assigning a QoS label for output classification
- Policing:
  - One-rate policing based on average rate and burst rate for a policer
  - Two-color policing that allows different actions for packets that conform to or exceed the rate
  - Aggregate policing for policers shared by multiple traffic classes
- Weighted Tail Drop (WTD) as the congestion-avoidance mechanism for managing the queue lengths and providing drop precedences for different traffic classifications
- Table maps for mapping DSCP, CoS, and IP precedence values
- Queuing and scheduling:
  - Shaped Round Robin (SRR) traffic shaping to mix packets from all queues to minimize traffic burst
  - Class-based traffic shaping to specify a maximum permitted average rate for a traffic class
  - Port shaping to specify the maximum permitted average rate for a port

  - Class-Based Weighted Fair Queuing (CBWFQ) to control bandwidth to a traffic class
  - WTD to adjust queue size for a specified traffic class
  - Low-latency priority queuing to allow preferential treatment to certain traffic
- Per-port, per-VLAN QoS to control traffic carried on a user-specified VLAN for a given interface. You can use hierarchical policy maps for per-VLAN classification and apply the per-port, per-VLAN hierarchical policy maps to trunk ports.
- Option to disable CPU protection to increase the available QoS policers from 45 to 64 per port (63 on every fourth port)

Layer 2 VPN Services

The CGR 2010 ESM provides the following Layer 2 VPN services:

- 802.1Q tunneling enables service providers to offer multiple point Layer 2 VPN services to customers
- Layer 2 Protocol Tunneling (L2PT) to enable customers to control protocols such as BPDU, CDP, VTP, LACP, and UDLD protocols to be tunneled across service-provider networks

Layer 3 Services

The CGR 2010 ESM provides the following Layer 3 services:

Note Layer 3 features are only available when the switch module is running the IP services image.

- HSRP Version 1 (HSRPv1) and HSRP Version 2 (HSRPv2) for Layer 3 router redundancy
- IP routing protocols for load balancing and for constructing scalable, routed backbones:
  - RIP Versions 1 and 2
  - OSPF
  - EIGRP
  - BGP Version 4
  - IS-IS dynamic routing
  - BFD protocol Bidirectional Forwarding Detection (BFD) Protocol to detect forwarding-path failures for OSPF, IS-IS, BGP, EIGRP, or HSRP routing protocols
- IP routing between VLANs (inter-VLAN routing) for full Layer 3 routing between two or more VLANs, allowing each VLAN to maintain its own autonomous data-link domain
- Policy-Based Routing (PBR) for configuring defined policies for traffic flows
- Static IP routing for manually building a routing table of network path information
- Equal-cost routing for load balancing and redundancy
- Internet Control Message Protocol (ICMP) and ICMP Router Discovery Protocol (IRDP) for using router advertisement and solicitation messages to discover the addresses of routers on directly attached subnets

- Protocol-Independent Multicast (PIM) for multicast routing within the network, allowing for devices in the network to receive the multicast feed requested, and for switches not participating in the multicast to be pruned. Includes support for PIM sparse mode (PIM-SM), PIM dense mode (PIM-DM), and PIM sparse-dense mode.
- Support for the SSM PIM protocol to optimize multicast applications, such as video
- Multicast Source Discovery Protocol (MSDP) for connecting multiple PIM-SM domains
- DHCP relay for forwarding UDP broadcasts, including IP address requests, from DHCP clients
- DHCP for IPv6 relay, client, server address assignment and prefix delegation
- IPv6 unicast routing capability for forwarding IPv6 traffic through configured interfaces using static routing, RIP, or OSPF
- IPv6 Default Router Preference (DRP) for improving the ability of a host to select an appropriate router
- Support for EIGRP IPv6, which utilizes IPv6 transport, communicates with IPv6 peers, and advertises IPv6 routes

Layer 3 VPN Services

The CGR 2010 ESM provides the following Layer 3 VPN services:

Note These features are available only when the switch module is running the IP services image.

- Multiple VPN Routing and Forwarding (multi-VRF) instances in customer edge devices (multi-VRF CE) to allow service providers to support multiple VPNs and overlap IP addresses between VPNs
- Multicast Virtual Routing and Forwarding (VRF) Lite for configuring multiple private routing domains for network virtualization and virtual private multicast networks
- VRF and EIGRP compatibility

Monitoring Features

The CGR 2010 ESM provides the following monitoring features:

- Switch Module LEDs that provide port and switch module-level status
- MAC address notification traps and RADIUS accounting for tracking users on a network by storing the MAC addresses that the switch module has learned or removed
- Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) for traffic monitoring on any port or VLAN
- SPAN and RSPAN support of Intrusion Detection Systems (IDS) to monitor, repel, and report network security violations
- Four groups (history, statistics, alarms, and events) of embedded RMON agents for network monitoring and traffic analysis
- Syslog facility for logging system messages about authentication or authorization errors, resource issues, and time-out events
- Layer 2 trace route to identify the physical path that a packet takes from a source device to a destination device

- Time Domain Reflector (TDR) to diagnose and resolve cabling problems on copper Ethernet 10/100 ports
- SFP module diagnostic management interface to monitor physical or operational status of an SFP module
- Online diagnostics to test the hardware functionality switch module while the switch module is connected to a live network
- On-board failure logging (OBFL) to collect information about the switch module and the power supplies connected to it
- Enhanced object tracking for HSRP clients (requires IP services image)
- IP Service Level Agreements (IP SLAs) support to measure network performance by using active traffic monitoring
- IP SLAs EOT to use the output from IP SLAs tracking operations triggered by an action such as latency, jitter, or packet loss for a standby router failover takeover
- EOT and IP SLAs EOT static route support to identify when a preconfigured static route or a DHCP route goes down
- IP SLAs for metro Ethernet using 802.1ag Ethernet Operation, Administration, and Maintenance (OAM) capability to validate connectivity, jitter, and latency in a metro Ethernet network
- Embedded event manager (EEM) for device and system management to monitor key system events and then act on them though a policy
- Support for EEM 3.2, which introduces event detectors for Neighbor Discovery, Identity, and MAC-Address-Table
- Support for the TWAMP standard for measuring round-trip network performance between any two devices that support the protocol

Default Settings after Initial Switch Module Configuration

The CGR 2010 ESM is designed for plug-and-play operation - you only need to assign basic IP information to the switch module and connect it to the other devices in your network. If you have specific network needs, you can change the interface-specific and system-wide settings.

Note For information about assigning an IP address by using the browser-based Express Setup program, see the *Cisco Connected Grid 10-Port Ethernet Switch Module Interface Card Getting Started Guide*. For information about assigning an IP address by using the CLI-based setup program, see Appendix A, "Initial Configuration with the CLI Setup Program."

If the CGR 2010 ESM is not configured, it operates with the default settings as shown in Table 1-3.

Table 1-3 Default Settings After Initial Switch Module Configuration

Feature	Default Setting	More information in...
Switch Module IP address, subnet mask, and default gateway	0.0.0.0	Chapter 4, "Assign the Switch Module IP Address and Default Gateway"
Domain name	None	

Table 1-3 Default Settings After Initial Switch Module Configuration (continued)

Feature	Default Setting	More information in...
Passwords	None defined	Chapter 6, "Administer the Switch Module"
TACACS+	Disabled	
RADIUS	Disabled	
System name and prompt	Switch	
NTP	Enabled	
DNS	Enabled	
MODBUS TCP	Disabled	Chapter 16, "MODBUS TCP Configuration"
802.1x	Disabled	See "Configuring IEEE 802.1x Port-Based Authentication" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/sw8021x.html)
DHCP		
DHCP client	Enabled	Chapter 4, "Assign the Switch Module IP Address and Default Gateway"
DHCP server	Enabled if the device acting as a DHCP server is configured and is enabled	
DHCP relay agent	Enabled (if the device is acting as a DHCP relay agent and is configured and enabled)	See "Configuring DHCP Features and IP Source Guard" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swdhcp82.html)
Port Parameters		
Port type	Gigabit Ethernet: NNI, Fast Ethernet ports: NNI	Chapter 8, "Interface Configuration"
Operating mode	Layer 2 (switchport)	
Port enable state	Enabled for NNIs; disabled for UNIs and ENIs	
Interface speed and duplex mode	Autonegotiate	
Auto-MDIX	Enabled	
Flow control	Off	
Command Macros	None configured	Chapter 10, "Smartports Macros Configuration"
VLANs		

Table 1-3 Default Settings After Initial Switch Module Configuration (continued)

Feature	Default Setting	More information in...
Default VLAN	VLAN 1	Chapter 11, "VLAN Configuration"
VLAN interface mode	Access	
VLAN type	UNI isolated	
Private VLANs	None configured	Chapter 12, "Private VLAN Configuration"
Dynamic ARP inspection	Disabled on all VLANs	See "Configuring Dynamic ARP Inspection" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swdynarp.html)
Tunneling		
802.1Q tunneling	Disabled	Chapter 13, "IEEE 802.1Q and Layer 2 Protocol Tunneling Configuration"
Layer 2 protocol tunneling	Disabled	
Spanning Tree Protocol		
STP	Rapid PVST+ enabled on NNIs in VLAN 1	See "Configuring STP" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swstp.html)
MSTP	Disabled (not supported on UNIs, can be configured on ENIs)	See "Configuring MSTP" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swmstp.html)
Optional spanning-tree features	Disabled (not supported on UNIs, but it can be configured on ENIs)	See "Configuring Optional Spanning-Tree Features" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swstpopt.html)
Resilient Ethernet Protocol	Not configured	See "Configuring Resilient Ethernet Protocol" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swrep.html)
Flex Links	Not configured	See "Configuring Flex Links and the MAC Address-Table Move Update Feature" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swflink.html)
DHCP Snooping	Disabled	
IP source guard	Disabled	See "Configuring DHCP Features and IP Source Guard" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swdhcp82.html)

Table 1-3 Default Settings After Initial Switch Module Configuration (continued)

Feature	Default Setting	More information in...
IGMP Snooping		
IGMP snooping	Enabled	See "Configuring IGMP Snooping and MVR" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swigmp.html)
IGMP filters	None applied	
IGMP querier	Disabled	
MVR	Disabled	
IGMP throttling	Deny	
Port-based Traffic Control		
Broadcast, multicast, and unicast storm control	Disabled	See "Configuring Port-Based Traffic Control" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swtrafc.html)
Protected ports	None defined	
Unicast and multicast traffic flooding	Not blocked	
Secure ports	None configured	
CDP	Enabled on NNIs, disabled on ENIs, not supported on UNIs	See "Configuring CDP" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swcdp.html)
LLDP	Disabled (not supported on UNIs)	See "Configuring LLDP and LLDP-MED" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swlldp.html)
UDLD	Disabled	See "Configuring UDLD" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swudld.html)
SPAN and RSPAN	Disabled	See "Configuring SPAN and RSPAN" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swspan.html)
RMON	Disabled	See "Configuring RMON" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swrmon.html)
Syslog messages	Enabled; displayed on the console.	See "Configuring System Message Logging" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swlog.html)
SNMP	Enabled; Version 1	See "Configuring SNMP" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swsnmp.html)

Table 1-3 Default Settings After Initial Switch Module Configuration (continued)

Feature	Default Setting	More information in...
ACLs	None configured	See "Configuring Network Security with ACLs" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swacl.html)
QoS	Not configured	Chapter 14, "Quality of Service Configuration"
EtherChannels	PortChannel 48	Chapter 9, "EtherChannel Configuration Between the Switch Module and the Host Router"
IP Unicast Routing		
IP routing and routing protocols	Disabled	See "Configuring IP Unicast Routing" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swiprout.html)
Multi-VRF-CE	Disabled	
HSRP groups (requires IP services image)	None configured	See "Configuring HSRP" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swhsrp.html)
Cisco IOS IP SLAs	Not configured	See "Configuring Cisco IOS IP SLAs Operations" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swipsla.html)
Enhanced object tracking	No tracked objects or list configured	See "Configuring Enhanced Object Tracking" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/sweot.html)
IP multicast routing (requires IP services image)	Disabled on all interfaces	See "Configuring IP Multicast Routing" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swmcast.html)
MSDP (requires IP services image)	Disabled	See "Configuring MSDP" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swmsdp.html)
Ethernet OAM		
CFM	Disabled globally, enabled per interface	See "Configuring Ethernet OAM, CFM, and E-LMI" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swoam.html)
E-LMI	Disabled globally	
Ethernet OAM protocol (802.3ah)	Disabled on all interfaces	

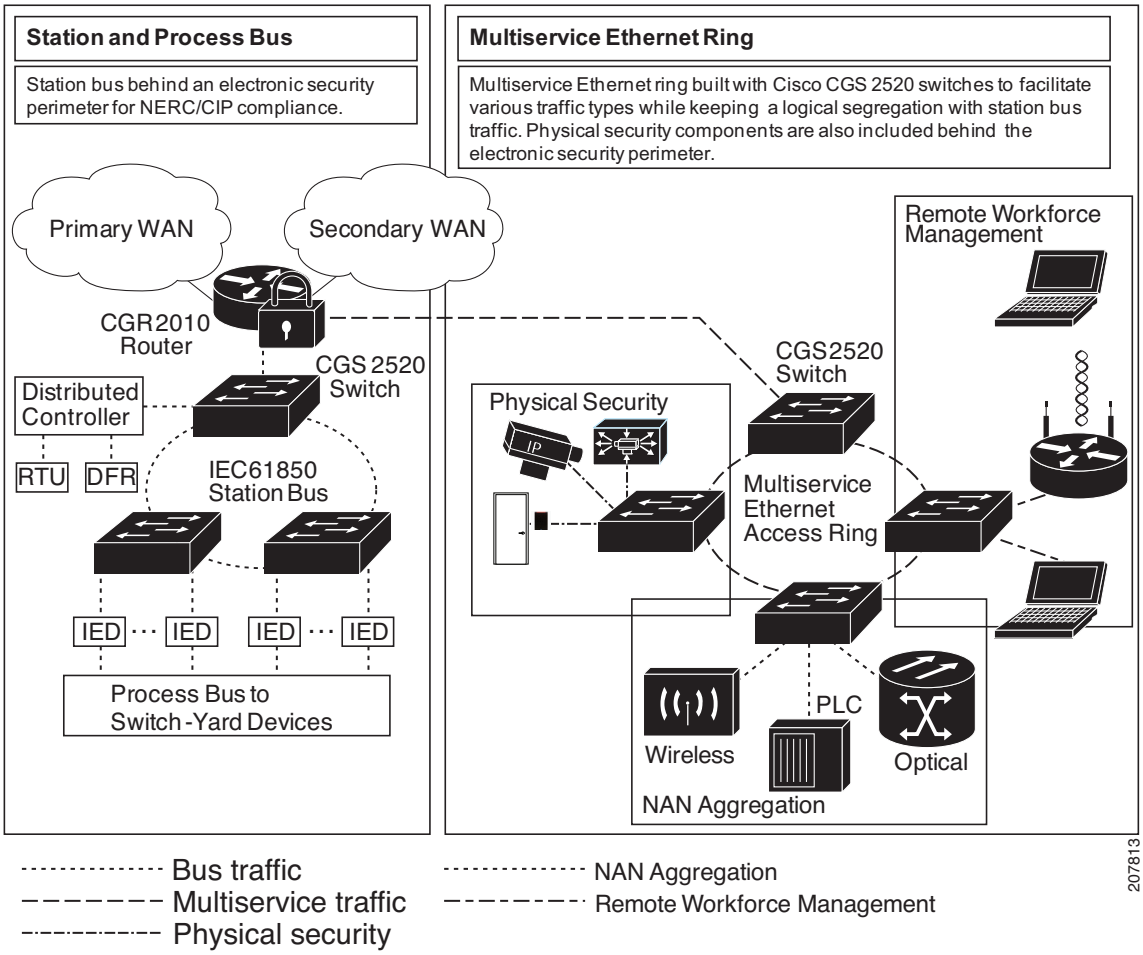
Utility Substation Application

Cisco CGR 2010 routers and the CGR 2010 ESM are designed for use in Transmission and Distribution (T&D) power substations. Figure 1-4 shows a partially redundant, multiservice configuration for deployment in a utility substation environment.

A substation router, such as a Cisco CGR 2010 router, defines the Electronic Security Perimeter (ESP) for the substation. The station bus network and multiservice network are located behind the substation router. The station bus network employs a ring topology for a resilient, redundant network and connects to different substation devices such as IEDs.

The multiservice network is virtually segmented from critical SCADA control traffic and supports services such as remote workforce management, physical security, and Field Area Network (FAN) aggregation. Advanced QoS capabilities support mission-critical substation traffic such as SCADA, and generic GOOSE messages, and ensures that substation network traffic is prioritized ahead of the multiservice network traffic.

Figure 1-4 CGR 2010 ESM in a Utility Substation Application



Where to Go Next

Before configuring the switch module module, review these chapters for startup information:

- Chapter 2, “Command Line Interface”
- Chapter 4, “Assign the Switch Module IP Address and Default Gateway”
- Chapter 5, “Cisco IOS Configuration Engine”

- Chapter 9, “EtherChannel Configuration Between the Switch Module and the Host Router”

Command Line Interface

This chapter describes the Cisco IOS Command Line Interface (CLI), how to use it to configure your switch module, and includes the following topics:

Understanding Command Modes

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

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

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

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

Table 2-1 describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode. The examples in the table use the hostname *Switch*.

Table 2-1 Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Start a session with the switch module	`Switch>`	Enter **logout** or **quit**	• Changes terminal settings • Performs basic tests • Displays system information
Privileged EXEC	While in user EXEC mode, enter the **enable** command	`Switch#`	Enter **disable** to exit	Verifies commands that you have entered. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the configure command	`Switch(config)#`	To exit to privileged EXEC mode, enter **exit** or **end**, or press **Ctrl-Z**	Configures parameters that apply to the entire switch module
VLAN configuration	While in global configuration mode, enter the **vlan** *vlan-id* command.	`Switch(config-vlan)#`	To exit to global configuration mode, enter the **exit** command. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Configures VLAN parameters
Interface configuration	While in global configuration mode, enter the **interface** command (with a specific interface)	`Switch(config-if)#`	To exit to global configuration mode, enter **exit**. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Configures parameters for the Ethernet ports. For information about defining interfaces, see the "Using Interface Configuration Mode" section on page 8-13. To configure multiple interfaces with the same parameters, see the "Configuring a Range of Interfaces" section on page 8-15.
Line configuration	While in global configuration mode, specify a line with the **line vty** or **line console** command	`Switch(config-line)#`	To exit to global configuration mode, enter **exit**. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Configures parameters for the terminal line

Understanding the CLI Help System

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

Table 2-2 CLI Help Summary

Command	Description
help	Brief description of the help system in any command mode

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

abbreviated-command-entry<**Tab**>	Complete a partial command name. For example:
	`Switch# sh conf<tab>`
	`Switch# show configuration`

?	List all commands available for a particular command mode. For example: `Switch> ?`
command **?**	List the associated keywords for a command. For example: `Switch> show ?`

command keyword **?**	List the associated arguments for a keyword. For example:
	`Switch(config)# cdp holdtime ?`
	`  <10-255> Length of time (in sec) that receiver must keep this packet`

Understanding Abbreviated Commands

You need to enter only enough characters for the switch module to recognize the command as unique. This example shows how to enter the **show configuration** privileged EXEC command in an abbreviated form:

```
Switch# show conf
```

Understanding *no* and *default* Forms of Commands

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

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

Understanding CLI Error Messages

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

Table 2-3 Common CLI Error Messages

Error Message	Meaning	How to Get Help
`% Ambiguous command: "show con"`	You did not enter enough characters for your switch module to recognize the command	Re-enter the command followed by a question mark (?) with a space between the command and the question mark.
`% Incomplete command`	You did not enter all the keywords or values required by this command	The possible keywords that you can enter with the command display.
`% Invalid input detected at '^' marker`	You entered the command incorrectly - he caret (^) marks the point of the error	

Using Command History

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

- Changing the Command History Buffer Size, page 2-4 (optional)
- Recalling Commands, page 2-5 (optional)
- Disabling the Command History Feature, page 2-5 (optional)

Changing the Command History Buffer Size

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

Beginning in privileged EXEC mode, enter this command to change the number of command lines that the switch module records during the current terminal session (range is from 0 to 256):

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

Beginning in line configuration mode, enter this command to configure the number of command lines the switch module records for all sessions on a particular line (range is from 0 to 256):

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

Recalling Commands

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

Table 2-4 Recalling Commands

Action[1]	Result
Press **Ctrl-P** or the Up arrow key	Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Press **Ctrl-N** or the Down arrow key	Return to more recent commands in the history buffer after recalling commands with **Ctrl-P** or the up arrow key. Repeat the key sequence to recall successively more recent commands.
show history	While in privileged EXEC mode, list the last several commands that you just entered. The number of commands that appear is controlled by the setting of the **terminal history** global configuration command and the **history** line configuration command.

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

Disabling the Command History Feature

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

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

To disable command history for the line, enter the **no history** line configuration command.

Using Editing Features

This section describes the editing features that can help you manipulate the command line.

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

Enabling and Disabling Editing Features

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

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

```
The arrow keys function only on ANSI-compatible terminals such as VT100s.Switch
(config-line)# no editing
```

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

```
Switch# terminal editing
```

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

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

Editing Commands Through Keystrokes

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

Table 2-5 Editing Commands through Keystrokes

Capability	Keystroke[1]	Description
Move around the command line to make changes or corrections	Press **Ctrl-B**, or press the left arrow key	Move the cursor back one character
	Press **Ctrl-F**, or press the right arrow key	Move the cursor forward one character
	Press **Ctrl-A**	Move the cursor to the beginning of the command line
	Press **Ctrl-E**	Move the cursor to the end of the command line
	Press **Esc B**	Move the cursor back one word
	Press **Esc F**	Move the cursor forward one word
	Press **Ctrl-T**	Transpose the character to the left of the cursor with the character located at the cursor
Recall commands from the buffer and paste them in the command line. The switch module provides a buffer with the last ten items that you deleted.	Press **Ctrl-Y**	Recall the most recent entry in the buffer

Table 2-5 Editing Commands through Keystrokes (continued)

Capability	Keystroke[1]	Description
	Press **Esc Y**	Recall the next buffer entry. The buffer contains only the last 10 items that you have deleted or cut. If you press **Esc Y** more than ten times, you cycle to the first buffer entry.
Delete entries if you make a mistake or change your mind	Press **Delete** or **Backspace**	Erase the character to the left of the cursor
	Press **Ctrl-D**	Delete the character at the cursor
	Press **Ctrl-K**	Delete all characters from the cursor to the end of the command line
	Press **Ctrl-U** or **Ctrl-X**	Delete all characters from the cursor to the beginning of the command line
	Press **Ctrl-W**	Delete the word to the left of the cursor
	Press **Esc D**	Delete from the cursor to the end of the word
Capitalize or lowercase words or capitalize a set of letters	Press **Esc C**	Capitalize at the cursor
	Press **Esc L**	Change the word at the cursor to lowercase
	Press **Esc U**	Capitalize letters from the cursor to the end of the word
Designate a particular keystroke as an executable command, perhaps as a shortcut	Press **Ctrl-V** or **Esc Q**	
Scroll down a line or screen on displays that are longer than the terminal screen can display. **Note** The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including **show** command output. You can use the **Return** and **Space** bar keystrokes whenever you see the More prompt.	Press **Return**	Scroll down one line

Table 2-5 Editing Commands through Keystrokes (continued)

Capability	Keystroke[1]	Description
	Press the **Space** bar	Scroll down one screen
Redisplay the current command line if the switch module suddenly sends a message to your screen.	Press **Ctrl-L** or **Ctrl-R**	Redisplay the current command line

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

Editing Command Lines That Wrap

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

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

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

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

```
Switch(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
Switch(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.25
Switch(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
Switch(config)# $108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
```

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

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

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

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

Searching and Filtering Output of *show* and *more* Commands

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

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

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

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

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

```
Switch# show interfaces | include protocol
Vlan1 is up, line protocol is up
Vlan10 is up, line protocol is down
GigabitEthernet0/1 is up, line protocol is down
GigabitEthernet0/2 is up, line protocol is up
```

Access the Switch Module from the Host Router

This chapter describes how to access the CGR 2010 ESM from the host CGR 2010 router, and contains the following topics:

Introduction

After the CGR 2010 ESM is installed on the router, you see a new Gigabit Ethernet interface *0/x/0* (where *x* is the slot number) recognized by the IOS. The output shown in Table 3-1 is taken after two switches are installed on the router:

```
Router1# show ip interface brief
```

Table 3-1 Output for Gigabit Ethernet Interface Recognized on the Switch Module

Interface	IP Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	60.60.60.1	YES	NVRAM	down	down
GigabitEthernet0/1	80.80.80.1	YES	manual	up	up
GigabitEthernet0/0/0	100.0.0.1	YES	manual	up	up
GigabitEthernet0/2/0	200.0.0.1	YES	NVRAM	up	up

The **service-module gigabitethernet 0/x/0 session** command is the privileged EXEC mode command used to console into the switch module from the host router.

You need to console into the switch module to configure it. To console into the switch module, you must configure an IP address on the internal backplane Gigabit Ethernet interface, that is, GE0/0/0 or GE0/2/0, connected to the switch module.

- If you try to console into the switch module without assigning an IP address, you receive the following error message:

```
Router# service-module gigabitethernet 0/2/0 session
IP address needs to be configured on interface GigabitEthernet0/2/0
```

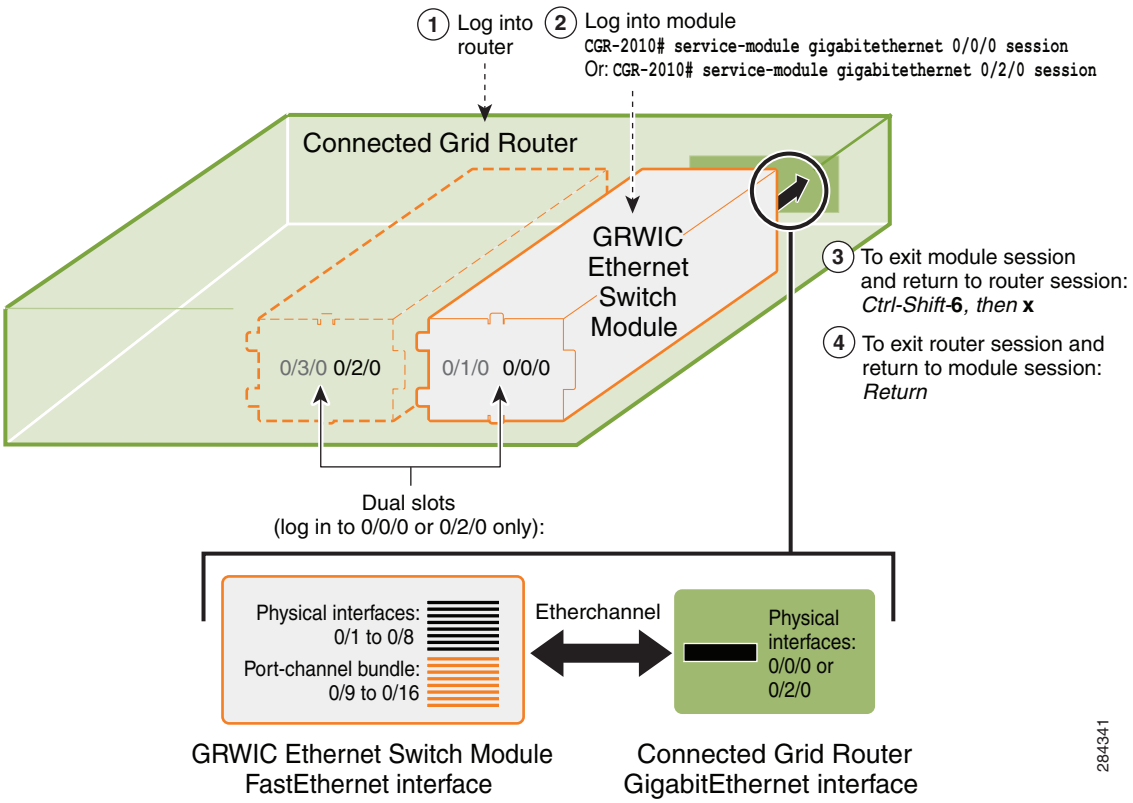
Accessing the Switch Module from the Host Router

This section covers the following topics:

Connected Grid Router and Ethernet Switch Module Relationship

The following diagram shows the relationship between the Connected Grid Router (CGR) and its GRWIC Ethernet Switch Module (ESM) and how to log into the CGR and into the ESM.

Figure 3-1 Connected Grid Router—Ethernet Switch Module Relationship



Example GRWICs

The following are example GRWICs:

Table 3-2 GRWIC Examples

GRWIC Type	Description
Copper model (Example: GRWIC-D-ES-2S-8PC)	Minimum-required OS version: 12.2(58)EY Interfaces (10 ports): • 8x 10/100 Fast Ethernet ports, • 1x dual-purpose port – (10/100/1000 Base-T copper RJ-45 and 100/1000 SFP fiber), • 1x 100/1000 SFP fiber-only port
SFP Fiber model (Example: GRWIC-D-ES-6S)	Minimum-required OS version: 12.2(58)EY Interfaces (6 ports): • 4x 100BASE-FX SFP-module ports, • 1x dual-purpose port (1x 10/100/1000Base-T copper RJ-45 port and 1x 100/1000 SFP fiber module port) (used to log into module) • 1x 100/1000 SFP fiber module port (used to log into module) • No physical console connection

Logging into a Module

Step 1 Configure the IP address of module.

```
CGR-2010(config)# interface g0/0/0
CGR-2010(config-if)# ip address 10.0.0.1 255.255.255.0
```

Step 2 Session into the module:

```
CGR-2010# service-module gigabitethernet 0/0/0 session
GRWIC-8PC>
```

Toggle Between Module Session and Router Session

After you have sessioned in to the module, you can toggle from the module session and to the router session by using the key combination of Cntrl-Shift-6, then x:

```
GRWIC-8PC>(Hit key combination Cntrl-Shift-6, then x.)
CGR-2010#
```

Similarly, you can toggle back to the module session by using the Return key:

```
CGR-2010# (Hit Return key.)
GRWIC-8PC>
```

To View OS Version on the Module

To view the OS version on the module, do the following:

```
GRWIC-8PC> enable
GRWIC-8PC# service-module gigabitethernet 0/0/0 status
```

To View OS Image Name of the Module

To view the name of the OS image on the module, do the following:

```
GRWIC-8PC> show version
```

Example image name: **grwicdes-ipservicesk9-mz.122-58.EY**

Note An IP services image provides Layer 3 services.

To View Interfaces on the Module

```
GRWIC-8PC> enable
GRWIC-8PC# show ip interface brief
```

Or:

```
GRWIC-8PC# show running configuration
```

Either command displays a list of the available physical interfaces and the virtual bundled interfaces.

Bundled Interfaces

Cisco IOS Release 12.3(13a)BC first introduced support for virtual interface bundling on the Cisco uBR10012 universal broadband router and the Cisco uBR10-MC5X20S/U/H Broadband Processing Engine (BPE), and the Cisco uBR7246VXR router. In prior Cisco IOS releases, cable interface bundling was limited to physical interfaces as master or slave interfaces, and **show** commands did not supply bundle information.

Why use bundled interfaces? Virtual interface bundling introduces these advantages:

- Uses bundle interface and bundle members instead of master and slave interfaces.
- Is virtually defined, as with IP loopback addresses, for example.
- Supports bundle information in multiple **show** commands.
- Prevents loss of connectivity on physical interfaces should there be a failure, problematic online insertion and removal (OIR) of one line card in the bundle, or erroneous removal of configuration on the master interface.
- Supports and governs the following Layer 3 settings for the bundle member interfaces:
  - IP address
  - IP helper-address
  - Source-verify and lease-timer functions

- Cable dhcp-giaddr (The giaddr field is set to the IP address of the DHCP client.)
- Protocol Independent Multicast (PIM)
- Access control lists (ACLs)
- Sub-interfaces

To Access the CGR 2010 ESM

To access the CGR 2010 ESM from the host router:

	Step	Command
Step 1	Log into the Cisco CGR 2010 router in privileged EXEC mode. Enter your password if prompted.	**Router> enable**
Step 2	Display the running interface of the router, which should have a Gigabit Ethernet interface representing the switch module.	Router# **show running interface gigabitethernet0/***<slot>***/0**
Step 3	Enter global configuration mode.	Router# **configure terminal**
Step 4	Enter interface configuration mode, and specifies the Gigabit interface used to access the switch module.	Router(config)# **interface gigabitethernet 0/***<slot>***/0**
Step 5	Configures the IP address and subnet mask for the interface.	Router(config-if)# **ip address 20.0.0.1 255.255.255.0**
Step 6	Enable the switch module port.	Router(config-if)# **no shutdown**
Step 7	Return to privileged EXEC mode.	Router(config-if)# **end**
Step 8	Establishes a session from the router over the internal backplane Gigabit Ethernet interface to the switch module.	**Router# service-module** *<interface>***<***slot/subslot/port***> session** **Example:** Router> **service-module gigabitethernet0/***<slot>***/0 session**
Step 9	After you execute the **service-module** *<interface>* **session** command, the switch module prompt appears and you have full access to the switch module.	Switch#

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

For information about configuring the switch module for SSH, see the "Configuring the Switch Module for Secure Shell" section on page 7-38. The switch module supports up to five simultaneous secure SSH sessions.

After you connect through the console port, through a Telnet session or through an SSH session, the user EXEC prompt appears on the management station.

Disconnecting from the Switch Module and Returning to the Host Router

To disconnect from the CGR 2010 ESM and return to the host Cisco CGR 2010 router:

	Step	Command
Step 1	Enter privileged EXEC mode on the switch module.	`Switch> enable`
Step 2	Display the brief version of the switch module configuration information.	`Switch# show ip interface brief`
Step 3	Press **<Ctrl+Shift+6>**, then press **x**. This sequence returns you to the router console while keeping the console session to the switch module intact and then exits the console session to the switch module.	`Switch# <Ctrl+Shift+6> x`
Step 4	Terminate the console session to the switch module.	`Router# disconnect`
Step 5	If not disconnected, press **Enter** to confirm the disconnect.	`Router# <Enter>`
Step 6	Display the status of all the vital components of the switch module. For example output, see Table 3-3 below.	`Router# service-module gigabitethernet 0/<slot>/0 status`

Service-Module Command Syntax

This section summarizes the syntax and command options for the **service-module** command.

Table 3-3 Service Module Command Syntax

Command	Function
`Router# service-module gigabitethernet0/<slot>/0 reload`	**reload**: Performs a graceful halt and reload of the switch module operating system. The configuration of the switch module is saved before reload.
Router# **service-module gigabitethernet0/**<*slot*>**/0 reload**	**reset**: Performs a hardware reset of the switch module. ⚠ **Caution** Use reset only to recover from shutdown or a failed state.

Table 3-3 Service Module Command Syntax (continued)

Command	Function
	 **Warning** **May lose data on the NVRAM, nonvolatile file system or an unsaved configuration.**
Router# **service-module gigabitethernet0/**<*slot*>**/0 session**	**session**: Establishes a session from the router over the internal backplane Gigabit Ethernet interface to the switch module.

Assign the Switch Module IP Address and Default Gateway

This chapter describes how to create the initial switch module configuration (for example, assigning the switch module module IP address and default gateway information) for the CGR 2010 ESM by using a variety of automatic and manual methods. It also describes how to modify the switch module startup configuration.

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

This chapter contains the following topics:

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

Understanding the Boot Process

To start your switch module, follow the procedures in the *Cisco Connected Grid 10-Port Ethernet Switch Module Interface Card Getting Started Guide* about installing and powering on the switch module, accessing the switch module from the host Cisco CGR 2010 router, and setting up the initial configuration (IP address, subnet mask, default gateway, secret and Telnet passwords, and so forth) of the switch module.

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 on
- 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 module

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 module has a 64 MB bootflash that can store two Cisco IOS software image and the configuration files.

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

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 on page 18-2 and "Recovering from a Lost or Forgotten Password" section on page 18-2.

Before you can assign switch module information, make sure you have connected a PC or terminal to the Cisco CGR 2010 router's console port, and configured the PC or terminal-emulation software baud rate and character format to match these of the router 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

Assigning Switch Module Information

You can assign IP information through the switch module setup program, through a DHCP server, or manually.

Use the switch module 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 Appendix A, "Initial Configuration with the CLI Setup Program."

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 module receives the dynamically assigned IP address and reads the configuration file.

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

These sections contain this configuration information:

Default Switch Module Information

Table 4-1 shows the default switch module information.

Table 4-1 Default Switch Module Information

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

Understanding DHCP-Based Autoconfiguration

DHCP provides configuration information to Internet hosts and internetworking devices. This protocol consists of two components: one for delivering configuration parameters from a DHCP server to a device and a mechanism for allocating network addresses to devices. DHCP is built on a client-server model, in which designated DHCP servers allocate network addresses and deliver configuration parameters to dynamically configured devices. The switch module can act as both a DHCP client and a DHCP server.

During DHCP-based autoconfiguration, your switch module (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 module. 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 module can be on the same LAN or on a different LAN than the switch module. If the DHCP server is running on a different LAN, you should configure a DHCP relay device between your switch module 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.

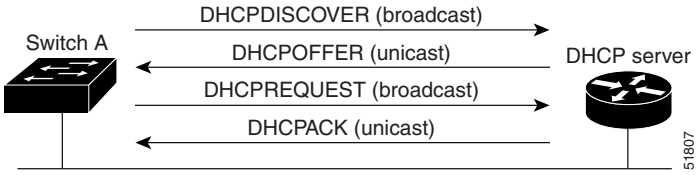
DHCP-based autoconfiguration replaces the BOOTP client functionality on your switch module.

DHCP Client Request Process

When you boot your switch module, the DHCP client is invoked and requests configuration information from a DHCP server when the configuration file is not present on the switch module. 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 4-1 shows the sequence of messages that are exchanged between the DHCP client and the DHCP server.

Figure 4-1 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 module receives depends on how you configure the DHCP server. For more information, see the "Configuring the TFTP Server" section on page 4-7.

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

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

A DHCP client might receive offers from multiple DHCP or BOOTP servers and can accept any of the offers; however, the client usually accepts the first offer it receives. The offer from the DHCP server is not a guarantee that the IP address is allocated to the client; however, the server usually reserves the address until the client has had a chance to formally request the address. If the switch module accepts replies from a BOOTP server and configures itself, the switch module broadcasts, instead of unicasts, TFTP requests to obtain the switch module 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 module) includes in its DCHPDISCOVER message an option 12 field used to request a hostname and other configuration parameters from the DHCP server. The configuration files on all clients are identical except for their DHCP-obtained hostnames.

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

Understanding DHCP-based Autoconfiguration and Image Update

You can use the DHCP image upgrade features to configure a DHCP server to download both a new image and a new configuration file to one or more switches in a network. This helps ensure that each new switch module 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 module. It does not over write the bootup configuration saved in the flash, until you reload the switch module.

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

Note To enable a DHCP auto-image update on the switch module, 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 module as a DHCP server, see the and the “Configuring DHCP” section of the “IP addressing and Services” section of the *Cisco IOS IP Configuration Guide, Release 12.2*.

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

Limitations and Restrictions

These are the limitations:

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

Configuring DHCP-Based Autoconfiguration

These sections contain this configuration information:

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

DHCP Server Configuration Guidelines

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

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

If you want the switch module 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 module) (required)

If you want the switch module 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 module 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 module is not configured. If the router IP address or the TFTP server name are not found, the switch module might send broadcast, instead of unicast, TFTP requests. Unavailability of other lease options does not affect autoconfiguration.

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

Configuring the TFTP Server

Based on the DHCP server configuration, the switch module attempts to download one or more configuration files from the TFTP server. If you configured the DHCP server to respond to the switch module 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 module 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 module 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 module'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 module 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:

- Configuration file named in the DHCP reply (the actual switch module configuration file)
- Network-confg or the cisconet.cfg file (known as the default configuration files)
- 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 module, or if it is to be accessed by the switch module through the broadcast address (which occurs if the DHCP server response does not contain all the required information described previously), a relay must be configured to forward the TFTP packets to the TFTP server. For more information, see the "Configuring the Relay Device" section on page 4-8. The preferred solution is to configure the DHCP server with all the required information.

Configuring the DNS

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

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 module. If it is on a different LAN, the switch module must be able to access it through a router.

Configuring the Relay Device

You must configure a relay device, also referred to as a *relay agent*, when a switch module sends broadcast packets that require a response from a host on a different LAN. Examples of broadcast packets that the switch module 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 4-2, configure the router interfaces as follows:

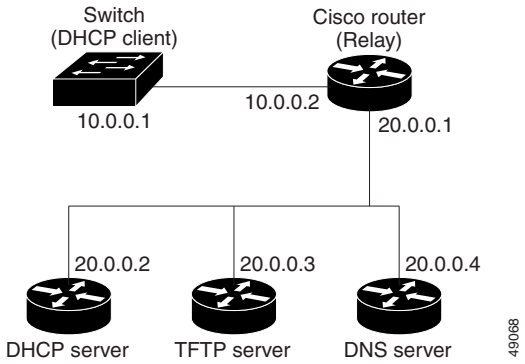
On interface 10.0.0.2:

```
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 4-2 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 module obtains its configuration information in these ways:

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

  The switch module receives its IP address, subnet mask, TFTP server address, and the configuration filename from the DHCP server. the switch module 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 module, but the TFTP server address is not provided in the DHCP reply (one-file read method).

  The switch module receives its IP address, subnet mask, and the configuration filename from the DHCP server. The switch module 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 module and provided in the DHCP reply. The configuration filename is not provided (two-file read method).

  The switch module receives its IP address, subnet mask, and the TFTP server address from the DHCP server. The switch module 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 module reads the cisconet.cfg file.)

  The default configuration file contains the hostnames-to-IP-address mapping for the switch module. The switch module 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 module uses the hostname in the DHCP reply. If the hostname is not specified in the DHCP reply, the switch module uses the default *Switch* as its hostname.

  After obtaining its hostname from the default configuration file or the DHCP reply, the switch module 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 module cannot read the network-confg, cisconet.cfg, or the hostname file, it reads the router-confg file. If the switch module cannot read the router-confg file, it reads the ciscortr.cfg file.

Note The switch module 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 4-3 shows a sample network for retrieving IP information by using DHCP-based autoconfiguration.

Figure 4-3 DHCP-Based Auto-Configuration Network Example

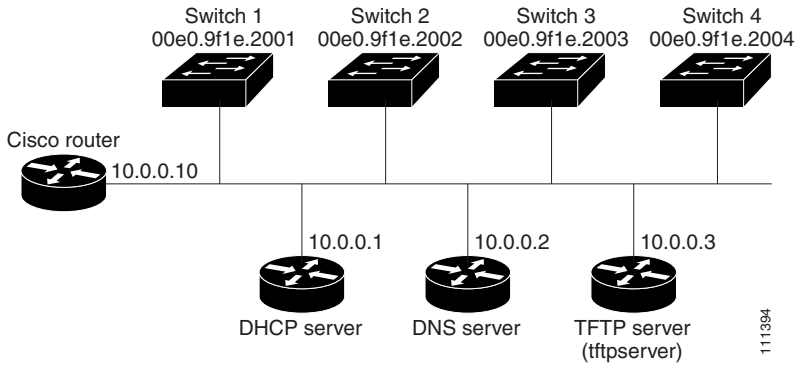


Table 4-2 shows the configuration of the reserved leases on the DHCP server.

Table 4-2 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 module based on its IP address. The base directory also contains a configuration file for each switch module (*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 4-3, 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.

Configuring the DHCP Auto Configuration and Image Update Features

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

Configuring DHCP Autoconfiguration (Only Configuration File)

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

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

This example shows how to configure a switch module as a DHCP server so that it will 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 gigabitethernet0/4
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1 255.255.255.0
Switch(config-if)# end
```

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

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

Note Before following the steps in this table, you must create a text file (for example, autoinstall_dhcp) that will be uploaded to the switch module. 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.

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

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

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

```
Switch# config terminal
Switch(config)# ip dhcp pool pool1
Switch(dhcp-config)# network 10.10.10.0 255.255.255.0
Switch(dhcp-config)# bootfile config-boot.text
Switch(dhcp-config)# default-router 10.10.10.1
Switch(dhcp-config)# option 150 10.10.10.1
Switch(dhcp-config)# option 125 hex
0000.0009.0a05.08661.7574.6f69.6e73.7461.6c6c.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

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

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enable autoconfiguration with a saved configuration.	**boot host dhcp**

	Step	Command
Step 3	(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.	**boot host retry timeout** *timeout-value*
Step 4	(Optional) Create warning messages to be displayed when you try to save the configuration file to NVRAM.	**banner config-save ^C** *warning-message* **^C**
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify the configuration.	**show boot**

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#
```

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

Beginning in privileged EXEC mode, follow these steps to manually assign IP information to a switch module virtual interface (SVI).

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	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.	**interface vlan** *vlan-id*
Step 3	Enter the IP address and subnet mask.	**ip address** *ip-address subnet-mask*
Step 4	Return to global configuration mode.	**exit**
Step 5	Enter the IP address of the next-hop router interface that is directly connected to the switch module where a default gateway is being configured. The default gateway receives IP packets with unresolved destination IP addresses from the switch module. Once the default gateway is configured, the switch module has connectivity to the remote networks with which a host needs to communicate. **Note** When your switch module is configured to route with IP, it does not need to have a default gateway set.	**ip default-gateway** *ip-address*
Step 6	Return to privileged EXEC mode.	**end**
Step 7	Verify the configured IP address.	**show interfaces vlan** *vlan-id*
Step 8	Verify the configured default gateway.	**show ip redirects**
Step 9	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To remove the switch module 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 module will be lost. To remove the default gateway address, use the **no ip default-gateway** global configuration command.

For information on setting the switch module system name, protecting access to privileged EXEC commands, and setting time and calendar services, see Chapter 6, “Administer the Switch Module.”

Checking and Saving the Running Configuration

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

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

Current configuration : 2010 bytes
```

```
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname switch
!
enable password cisco
!
no aaa new-model
ip subnet-zero
no ip domain-lookup
!
table-map test
  default copy
!
no file verify auto
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 2,10
!
class-map match-all test1
class-map match-all class2
class-map match-all class1
!
!
policy-map test
  class class1
   police cir percent 30
policy-map test2
  class class2
   police cir 8500 bc 1500
policy-map test3
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
  shutdown
!
interface FastEthernet0/3
  shutdown
!
interface FastEthernet0/4
  shutdown
!
interface FastEthernet0/5
  shutdown
!
interface FastEthernet0/6
  shutdown
!
interface FastEthernet0/7
  shutdown

<output truncated>

interface GigabitEthernet0/1
```

```
  port-type nni
!
interface GigabitEthernet0/2
  port-type nni
!
interface Vlan1
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
!
interface Vlan10
  ip address 192.168.1.76 255.255.255.0
!
ip default-gateway 192.168.1.3
no ip http server
ip classless
!
!
!
control-plane
!
!
line con 0
  session-timeout 120
  exec-timeout 120 0
  speed 115200
line vty 0 4
  password cisco
  no login
line vty 5 15
  no login
!
!
end
```

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

```
Switch# copy running-config startup-configuration
Destination filename [startup-configuration]?
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-configuration** or **more startup-configuration** privileged EXEC command.

For more information about alternative locations from which to copy the configuration file, see Appendix B, "Cisco IOS File System, Configuration Files, and Software Images."

Modifying the Startup Configuration

This section describes how to modify the startup configuration, and contains the following sections:

- Booting a Specific Software Image, page 4-20
- Controlling Environment Variables, page 4-21

See also Appendix B, "Cisco IOS File System, Configuration Files, and Software Images," for information about switch module configuration files.

Default Boot Configuration

Table 4-3 shows the default boot configuration.

Table 4-3 Default Boot Configuration

Feature	Default Setting
Operating system software image	The switch module attempts to automatically boot the system using information in the BOOT environment variable. If the variable is not set, the switch module 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 switch modulees use the *config.text* file stored on the system board in flash memory. A new switch module has no configuration file.

Automatically Downloading a Configuration File

You can automatically download a configuration file to your switch module by using the DHCP-based autoconfiguration feature. For more information, see the "Understanding DHCP-Based Autoconfiguration" section on page 4-3.

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.

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

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	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.	**boot config-file flash:/***file-url*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entries. The **boot config-file** global configuration command changes the setting of the CONFIG_FILE environment variable.	**show boot**
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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

Booting Manually

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

Beginning in privileged EXEC mode, follow these steps to configure the switch module to manually boot during the next boot cycle:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enable the switch module to manually boot during the next boot cycle.	**boot manual**
Step 3	Return to privileged EXEC mode.	**end**

	Step	Command
Step 4	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 module is in boot loader mode, 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.	**show boot**
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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

Booting a Specific Software Image

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

Beginning in privileged EXEC mode, follow these steps to configure the switch module to boot a specific image during the next boot cycle:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Configure the switch module 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.	**boot system** *filesystem***:/***file-url*
Step 3	Return to privileged EXEC mode.	**end**

	Step	Command
Step 4	Verify your entries. The **boot system** global command changes the setting of the BOOT environment variable. During the next boot cycle, the switch module attempts to automatically boot the system using information in the BOOT environment variable.	**show boot**
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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

Controlling Environment Variables

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

Environment variables that have values are stored in flash memory outside of the flash file system.

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

Environment variables store two kinds of data:

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

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

Note For complete syntax and usage information for the boot loader commands and environment variables, see the command reference for this release.

Table 4-4 describes the function of the most common environment variables.

Table 4-4 Environmental 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 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** f*ilesystem:/file-url* ... Specifies the Cisco IOS image 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 module 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 module from the boot loader mode.	**boot manual** Enables manually booting the switch module during the next boot cycle and changes the setting of the MANUAL_BOOT environment variable. The next time you reboot the system, the switch module 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.

Scheduling a Reload of the Software Image

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

Note A scheduled reload must take place within approximately 24 days.

Configuring a Scheduled Reload

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

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

  This command schedules a reload of the software to take affect 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.

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

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

Note Use the **at** keyword only if the switch module 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 module. To schedule reloads across several switches to occur simultaneously, the time on each switch module must be synchronized with NTP.

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

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

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

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

```
Switch# reload at 19:30
Reload scheduled for 19:30:00 UTC Fri June 3 2011 (in 2 hours and 25 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 module, 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).

Cisco IOS Configuration Engine

This chapter describes how to use the Cisco Configuration Engine to configure the CGR 2010 ESM.

Note For complete configuration information for the Cisco Configuration Engine, go to http://www.cisco.com/en/US/products/sw/netmgtsw/ps4617/tsd_products_support_series_home.html

For complete syntax and usage information for the commands used in this chapter, go to the *Cisco IOS Network Management Command Reference, Release 12.4* at http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_book.html

This chapter consists of the following topics:

Understanding Cisco Configuration Engine Software

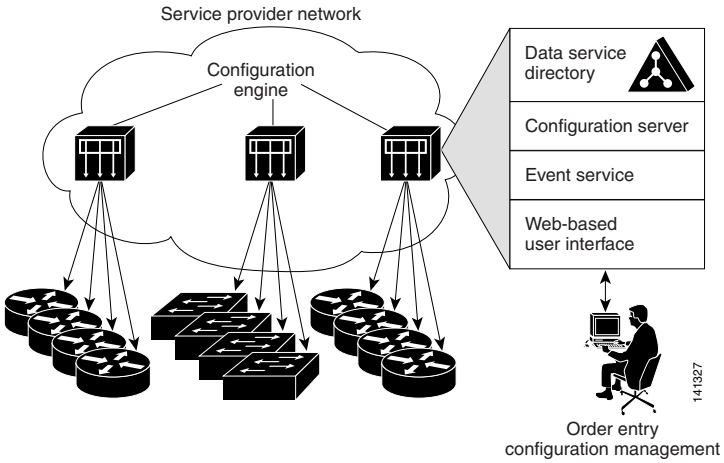
The Cisco Configuration Engine is network management software that acts as a configuration service for automating the deployment and management of network devices and services (see Figure 5-1). Each Configuration Engine manages a group of Cisco devices (switches and routers) and the services that they deliver, storing their configurations and delivering them as needed. The Configuration Engine automates initial configurations and configuration updates by generating device-specific configuration changes, sending them to the device, executing the configuration change, and logging the results.

The Configuration Engine supports standalone and server modes and has these Cisco Networking Services (CNS) components:

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

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

Figure 5-1 Configuration Engine Architectural Overview



These sections contain the following conceptual information:

- Configuration Service, page 5-2
- Event Service, page 5-2
- About the CNS IDs and Device Hostnames, page 5-3

Configuration Service

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

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

The configuration server is a web server that uses configuration templates and the device-specific configuration information stored in the embedded (standalone mode) or remote (server mode) directory.

Configuration templates are text files containing static configuration information in the form of CLI commands. In the templates, variables are specified using Lightweight Directory Access Protocol (LDAP) URLs that reference the device-specific configuration information stored in a directory.

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

Event Service

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

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

NameSpace Mapper

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

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

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

About the CNS IDs and Device Hostnames

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

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

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

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

ConfigID

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

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

DeviceID

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

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

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

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

Hostname and DeviceID

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

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

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

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

Using Hostname, DeviceID and ConfigID

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

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

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

Note For more information about running the setup program on the Configuration Engine, see the Configuration Engine setup and configuration guide at http://www.cisco.com/en/US/products/sw/netmgtsw/ps4617/prod_installation_guides_list.html

Understanding Cisco IOS Agents

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

Initial Configuration

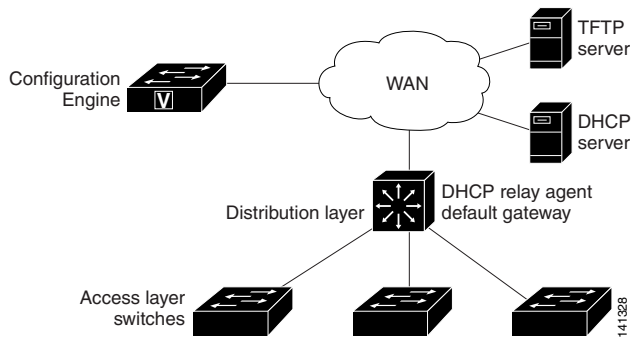
When the switch module first comes up, it attempts to get an IP address by broadcasting a DHCP request on the network. Assuming there is no DHCP server on the subnet, the distribution switch module acts as a DHCP relay agent and forwards the request to the DHCP server. On receiving the request, the DHCP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

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

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

Figure 5-2 shows a sample network configuration for retrieving the initial bootstrap configuration file by using DHCP-based autoconfiguration.

Figure 5-2 Initial Configuration Overview



Incremental (Partial) Configuration

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

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

Synchronized Configuration

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

Configuring Cisco IOS Agents

The Cisco IOS agents embedded in the switch module Cisco IOS software allow the switch module to be connected and automatically configured as described in the "Enabling Automated CNS Configuration" section on page 5-6. If you want to change the configuration or install a custom configuration, see these sections for instructions:

- Enabling the CNS Event Agent, page 5-7
- Enabling the Cisco CNS Configuration Agent, page 5-9
- Upgrading Devices with Cisco CNS Image Agent, page 5-11

Enabling Automated CNS Configuration

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

Table 5-1 Prerequisites for Enabling Automatic Configuration

Device	Required Configuration
Access switch module	Factory default (no configuration file)
Distribution switch module	• IP helper address • Enable DHCP relay agent • IP routing (if used as default gateway)
DHCP server	• IP address assignment • TFTP server IP address • Path to bootstrap configuration file on the TFTP server • Default gateway IP address

Table 5-1 Prerequisites for Enabling Automatic Configuration (continued)

Device	Required Configuration
TFTP server	• A bootstrap configuration file that includes the CNS configuration commands that enable the switch module to communicate with the Configuration Engine • The switch module configured to use either the switch module MAC address or the serial number (instead of the default hostname) to generate the ConfigID and EventID • The CNS event agent configured to push the configuration file to the switch module
CNS Configuration Engine	One or more templates for each type of device, with the ConfigID of the device mapped to the template.

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

Enabling the CNS Event Agent

Note You must enable the CNS Event Agent on the switch module before you enable the CNS configuration agent.

Beginning in privileged EXEC mode, follow these steps to enable the CNS event agent on the switch module:

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

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

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

```
Switch(config)# cns event 10.180.1.27 keepalive 120 10
```

Enabling the Cisco CNS Configuration Agent

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

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

Enabling an Initial Configuration

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

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter CNS template connect configuration mode, and specify the name of the CNS connect template.	**cns template connect** *name*
Step 3	Enter a command line for the CNS connect template. Repeat this step for each command line in the template.	**cli** *config-text*
Step 4	Repeat Steps 2 to 3 to configure another CNS connect template.	
Step 5	Return to global configuration mode.	**exit**

To disable the CNS Cisco IOS agent, use the **no cns config initial** {*ip-address* | *hostname*} global configuration command.

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

```
Switch(config)# cns template connect template-dhcp
Switch(config-tmpl-conn)# cli ip address dhcp
Switch(config-tmpl-conn)# exit
Switch(config)# cns template connect ip-route
Switch(config-tmpl-conn)# cli ip route 0.0.0.0 0.0.0.0 ${next-hop}
Switch(config-tmpl-conn)# exit
Switch(config)# cns connect dhcp
Switch(config-cns-conn)# discover interface gigabitethernet
Switch(config-cns-conn)# template template-dhcp
Switch(config-cns-conn)# template ip-route
Switch(config-cns-conn)# exit
Switch(config)# hostname RemoteSwitch
RemoteSwitch(config)# cns config initial 10.1.1.1 no-persist
```

This example shows how to configure an initial configuration on a remote switch module when the switch module IP address is known. The Configuration Engine IP address is 172.28.129.22.

```
Switch(config)# cns template connect template-dhcp
Switch(config-tmpl-conn)# cli ip address dhcp
Switch(config-tmpl-conn)# exit
Switch(config)# cns template connect ip-route
Switch(config-tmpl-conn)# cli ip route 0.0.0.0 0.0.0.0 ${next-hop}
```

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

Enabling a Partial Configuration

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

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enable the configuration agent, and initiate a partial configuration. • For {*ip-address* | *hostname*}, enter the IP address or the hostname of the configuration server. • (Optional) For *port-number*, enter the port number of the configuration server. The default port number is 80. • (Optional) Enter **source** *ip-address* to use for the source IP address. **Note** Though visible in the command-line help string, the **encrypt** keyword is not supported.	**cns config partial** {*ip-address* | *hostname*} [*port-number*] [**source** *ip-address*]
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify information about the configuration agent.	**show cns config stats** or **show cns config outstanding**
Step 5	Verify your entries.	**show running-config**
Step 6	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To disable the Cisco IOS agent, use the **no cns config partial** {*ip-address* | *hostname*} global configuration command. To cancel a partial configuration, use the **cns config cancel** privileged EXEC command.

Upgrading Devices with Cisco CNS Image Agent

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

You can use the Image Agent to download one or more devices. The switch modulees must have the Image Agent running on them.

Prerequisites for the CNS Image Agent

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

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

Restrictions for the CNS Image Agent

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

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

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

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

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

	Step	Command
Step 1	Enter global configuration mode	**configure terminal**
Step 2	Enter the IP address and the hostname of the event gateway.	**ip host** {*ip-address*} {*hostname*}
Step 3	Specify a trusted server for CNS agent.	**cns trusted-server all-agents** {*hostname*}

	Step	Command
Step 4	Disable AAA authentication on the event gateway.	**no cns aaa enable cns event** {*ip-address*} {*port number*}
Step 5	Specify the number of times to retry and download the image.	**cns image retry** {*number*}
Step 6	Download the image from the server to the switch module.	**cns image server** {*ip-address*} **status** {*ip-address*}
Step 7	Return to privileged EXEC mode.	**end**

Note This example shows how to upgrade a switch module from a server with the address of **172.20.249.20:**

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

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

Displaying CNS Configuration

You can use the privileged EXEC commands in Table 5-2 to display CNS configuration information.

Table 5-2 Displaying CNS Configuration

Command	Description
show cns config connections	Displays the status of the CNS Cisco IOS agent connections.
show cns config outstanding	Displays information about incremental (partial) CNS configurations that have started but are not yet completed.
show cns config stats	Displays statistics about the Cisco IOS agent.
show cns event connections	Displays the status of the CNS event agent connections.
show cns event stats	Displays statistics about the CNS event agent.
show cns event subject	Displays a list of event agent subjects that are subscribed to by applications.

Administer the Switch Module

This chapter describes how to perform one-time operations to administer the CGR 2010 ESM, as well as how to monitor the switch module's temperature and configure the temperature yellow threshold. This chapter contains the following topics:

Managing the System Time and Date

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

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

These sections contain the following configuration information:

Understanding the System Clock

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

The system clock can then be set from these sources:

- Network Time Protocol
- Manual configuration

The system clock can provide time to these services:

- User **show** commands
- Logging and debugging messages

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

The system clock keeps track of whether the time is *authoritative* or not (that is, whether it has been set by a time source considered to be authoritative). If it is not authoritative, the time is available only for display purposes and is not redistributed. For configuration information, see the "Configuring Time and Date Manually" section on page 6-12.

Understanding the Network Time Protocol

The Network Time Protocol (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.

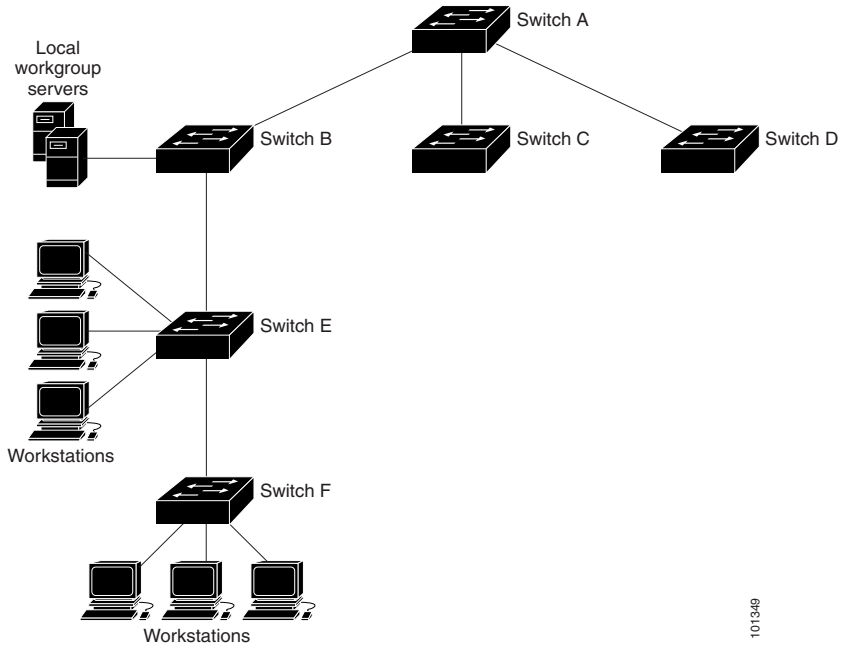
The communications between devices running NTP (known as *associations*) are usually statically configured; each device is given the IP address of all devices with which it should form associations. Accurate timekeeping is possible by exchanging NTP messages between each pair of devices with an association. 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 6-1 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 switch module, Switch B and Switch F.

Figure 6-1 Typical NTP Network Configuration



If the network is isolated from the Internet, Cisco's implementation of NTP allows a device to act as if it is synchronized through NTP, when in fact it has learned the time by using other means. Other devices then synchronize to that device through NTP.

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

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

Configuring the Network Time Protocol

The switch module 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 module 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.

These sections contain this configuration information:

Default NTP Configuration

Table 6-1 shows the default NTP configuration.

Table 6-1 Default NTP Configuration

Feature	Default Setting
NTP authentication	Disabled - no authentication key is specified
NTP peer or server associations	None configured
NTP broadcast service	Disabled; no interface sends or receives NTP broadcast packets
NTP access restrictions	No access control is specified
NTP packet source IP address	The source address is set by the outgoing interface

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

Configuring NTP Authentication

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

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

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enable the NTP authentication feature, which is disabled by default.	**ntp authenticate**
Step 3	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 module 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.	**ntp authentication-key** *number* **md5** *value*

	Step	Command
Step 4	Specify one or more key numbers (defined in Step 3) that a peer NTP device must provide in its NTP packets for this switch module 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 module to a device that is not trusted.	**ntp trusted-key** *key-number*
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify your entries.	**show running-config**
Step 7	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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

This example shows how to configure the switch module 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 module 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 module synchronizes to the other device, and not the other way around).

Beginning in privileged EXEC mode, follow these steps to form an NTP association with another device:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Configure the switch module system clock to synchronize a peer or to be synchronized by a peer (peer association). or Configure the switch module 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 switch moduleing back and forth between peers and servers.	**ntp peer** *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**] or **ntp server** *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**]
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entries.	**show running-config**
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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

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

This example shows how to configure the switch module 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 module 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 module can send NTP broadcast packets to a peer so that the peer can synchronize to it. the switch module can also receive NTP broadcast packets to synchronize its own clock. This section provides procedures for both sending and receiving NTP broadcast packets.

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

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the interface to send NTP broadcast packets, and enter interface configuration mode.	**interface** *interface-id*
Step 3	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.	**no shutdown**
Step 4	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 module.	**ntp broadcast** [**version** *number*] [**key** *keyid*] [*destination-address*]
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify your entries.	**show running-config**

	Step	Command
Step 7	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**
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.

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

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

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

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

To disable an interface from receiving NTP broadcast packets, use the **no ntp broadcast client** interface configuration command. To change the estimated round-trip delay to the default, use the **no ntp broadcastdelay** global configuration command.

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

```
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 6-9
- Disabling NTP Services on a Specific Interface, page 6-10

Creating an Access Group and Assigning a Basic IP Access List

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

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	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 module to synchronize to the remote device. • **peer**—Allows time requests and NTP control queries and allows the switch module to synchronize to the remote device. For *access-list-number*, enter a standard IP access list number from 1 to 99.	**ntp access-group** {**query-only** | **serve-only** | **serve** | **peer**} *access-list-number*
Step 3	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 module. • (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.	**access-list** *access-list-number* **permit** *source* [*source-wildcard*]
Step 4	Return to privileged EXEC mode.	**end**

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

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

- **peer**—Allows time requests and NTP control queries and allows the switch module to synchronize itself to a device whose address passes the access list criteria.
- **serve**—Allows time requests and NTP control queries, but does not allow the switch module to synchronize itself to a device whose address passes the access list criteria.
- **serve-only**—Allows only time requests from a device whose address passes the access list criteria.
- **query-only**—Allows only NTP control queries from a device whose address passes the access list criteria.

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

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

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

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

Disabling NTP Services on a Specific Interface

NTP services are enabled on all interfaces by default.

Beginning in privileged EXEC mode, follow these steps to disable NTP packets from being received on an interface:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and specify the interface to disable.	**interface** *interface-id*
Step 3	Enable the port, if necessary. By default, UNIs and enhanced network interfaces (ENIs) are disabled, and NNIs are enabled.	**no shutdown**
Step 4	Disable NTP packets from being received on the interface. By default, all interfaces receive NTP packets.	**ntp disable**
Step 5	Return to privileged EXEC mode.	**end**

	Step	Command
Step 6	Verify your entries.	**show running-config**
Step 7	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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

Configuring the Source IP Address for NTP Packets

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

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

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

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 6-5.

Displaying the NTP Configuration

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

- **show ntp associations** [**detail**]
- **show ntp status**

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

Configuring Time and Date Manually

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

These sections contain this configuration information:

Setting the System Clock

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

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

	Step	Command
Step 1	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).	**clock set** *hh*:*mm*:*ss day month year* or **clock set** *hh*:*mm*:*ss month day year*

This example shows how to manually set the system clock to 1:30 P.M. on September 30, 2010:

```
Switch# clock set 13:30:00 30 September 2010
```

Displaying the Time and Date Configuration

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

The system clock keeps an *authoritative* flag that shows whether the time is authoritative (believed to be accurate). If the system clock has been set by a timing source such as NTP, the flag is set. If the time is not authoritative, it is used only for display purposes. Until the clock is authoritative and the *authoritative* flag is set, the flag prevents peers from synchronizing to the clock when the peers' time is invalid.

The symbol that precedes the **show clock** display has this meaning:

- *—Time is not authoritative.

- (blank)—Time is authoritative.
- .—Time is authoritative, but NTP is not synchronized.

Configuring the Time Zone

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

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Set the time zone. The switch module 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.	**clock timezone** *zone hours-offset* [*minutes-offset*]
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entries.	**show running-config**
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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

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

Configuring Summer Time (Daylight Saving Time)

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

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

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

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

```
Switch(config)# clock summer-time PDT recurring 1 Sunday June 2:00 last Sunday September
2:00
```

Beginning in privileged EXEC mode, follow these steps if summer time in your area does not follow a recurring pattern (configure the exact date and time of the next summer time events):

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

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

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

This example shows how to set summer time to start on June 20, 2010, at 02:00, and end on September 23, 2010, at 02:00:

```
Switch(config)# clock summer-time pdt date 20 June 2010 2:00 23 September 2010 2:00
```

Configuring a System Name and Prompt

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

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

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

These sections contain this configuration information:

Default System Name and Prompt Configuration

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

Configuring a System Name

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

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	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 have as interior characters only letters, digits, and hyphens. Names can be up to 63 characters.	**hostname** *name*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entries.	**show running-config**
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-confi**g

When you set the system name, it is also used as the system prompt. To return to the default hostname, use the **no hostname** global configuration command.

Understanding DNS

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

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

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

These sections contain this configuration information:

Default DNS Configuration

Table 6-2 shows the default DNS configuration.

Table 6-2 Default DNS Configuration

Feature	Default Setting
DNS enable state	Enabled
DNS default domain name	None configured
DNS servers	No name server addresses are configured

Setting Up DNS

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

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Define a default domain name that the software uses to complete unqualified hostnames (names without a dotted-decimal domain name). Do not include the initial period that separates an unqualified name from the domain name. At boot time, no domain name is configured; however, if the switch module 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).	**ip domain-name** *name*

	Step	Command
Step 3	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 module sends DNS queries to the primary server first. If that query fails, the backup servers are queried.	**ip name-server** *server-address1* [*server-address2 ... server-address6*]
Step 4	(Optional) Enable DNS-based hostname-to-address translation on your switch module. This feature is enabled by default. If your network devices require connectivity with devices in networks for which you do not control name assignment, you can dynamically assign device names that uniquely identify your devices by using the global Internet naming scheme (DNS).	**ip domain-lookup**
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify your entries.	**show running-config**
Step 7	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

If you use the switch module IP address as its hostname, the IP address is used and no DNS query occurs. If you configure a hostname that contains no periods (.), a period followed by the default domain name is appended to the hostname before the DNS query is made to map the name to an IP address. The default domain name is the value set by the **ip domain-name** global configuration command. If there is a period (.) in the hostname, the Cisco IOS software looks up the IP address without appending any default domain name to the hostname.

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

Displaying the DNS Configuration

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

Creating a Banner

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

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

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

These sections contain this configuration information:

Default Banner Configuration

The message of the day and login banners are not configured by default.

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 module.

Beginning in privileged EXEC mode, follow these steps to configure a message of the day login banner:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	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.	**banner motd** *c message c*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entries.	**show running-config**
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To delete the message of the day banner, use the **no banner motd** global configuration command.

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

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

```
Switch(config)#
```

This example shows the banner that appears from the previous configuration:

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

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

User Access Verification

Password:
```

Configuring a Login Banner

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

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

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	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.	**banner login** *c message c*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entries.	**show running-config**
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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

This example shows how to configure a login banner for the switch module 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)#
```

Monitoring Temperature and Configuring the Yellow Threshold

The CGR 2010 ESM includes sensors that measure and monitor the status and internal temperature of critical components. Internal component temperatures are measured for the central processor, internal components, and interface cards.

The measured temperature is compared to predetermined threshold limits and, if the temperature does not fall within the limits, the information is recorded and a warning sent to the system administrator by means of Simple Network Management Protocol (SNMP) traps until the temperature falls back to its normal range.

- Use the **show env temperature status** privileged EXEC command to display the current temperature value, state, and thresholds of the switch module's CPU and Ethernet board (see Table 6-3 below). The temperature value is the temperature in the switch module (not the external temperature). If the temperature exceeds the threshold, a warning message is sent.
- You can configure the yellow threshold level (in Celsius) by using the **system env temperature threshold yellow** *value* global configuration command to set the difference between the yellow and red thresholds. You cannot configure the green or red thresholds (see "Configuring the Yellow Threshold" below for details).

Temperature Show Commands

The switch module monitors the temperature conditions to determine the health of the power supplies. The temperature value is the temperature in the switch module (not the external temperature).

Table 6-3 describes the **Show** commands that monitor the switch module's temperature:

Table 6-3 Temperature Show Commands

Command	Function
Switch# **show env** *all* | *temperature status*	• *all*: Displays all environmental monitor parameters and enhanced to show the history data. • *temperature status*: Shows temperature status and threshold levels of the switch module's CPU and Ethernet board.

Configuring the Yellow Threshold

You cannot configure the green and red thresholds but you can configure the yellow threshold.

Use the **system env temperature threshold yellow** *value* global configuration command to specify the difference between the yellow and red threshold values and to configure the yellow threshold (in Celsius). The range is 20 to 25. The default value is 20.

For example, if the red threshold is 60º C and you want to configure the yellow threshold as 51º C (a 9º difference), set the 9º difference between the red and yellow thresholds by using the **system env temperature threshold yellow 9** command.

Use the **no** form of this command to return to the default value.

The default yellow thresholds differ for the switch module's Copper and SFP models (see Table 6-4).

Table 6-4 Default Yellow and Red Thresholds for Copper and SFP Models

Model	Default Yellow Threshold	Default Red Threshold
GRWIC-D-ES-2S-8PC (Copper model)	85ºC	105º C
GRWIC-D-ES-6S (SFP model)	90º C	105º C

Managing the MAC Address Table

The MAC address table contains address information that the switch module 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 module 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 module resets.

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

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

These sections contain this configuration information:

Building the Address Table

With multiple MAC addresses supported on all ports, you can connect any port on the switch module to individual workstations, repeaters, switches, routers, or other network devices. The switch module 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 module 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 module maintains an address table for each VLAN, and STP can accelerate the aging interval on a per-VLAN basis.

The switch module sends packets between any combination of ports, based on the destination address of the received packet. Using the MAC address table, the switch module 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 module 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 Chapter 12, “Private VLAN Configuration.”

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 module by controlling which VLANs, and which ports, can learn MAC addresses.

Before you disable MAC address learning, be sure that you are familiar with the network topology and the switch module system configuration. Disabling MAC address learning on a VLAN could cause flooding in the network. See the “Disabling MAC Address Learning on a VLAN” section on page 6-32 for more information.

Default MAC Address Table Configuration

Table 6-5 shows the default MAC address table configuration.

Table 6-5 Default MAC Address Table Configuration

Feature	Default Setting
Aging time	300 seconds
Dynamic addresses	Automatically learned
Static addresses	None configured

Changing the Address Aging Time

Dynamic addresses are source MAC addresses that the switch module 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 module 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 module performance.

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

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	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.	**mac address-table aging-time** [**0** | *10-1000000*] [**vlan** *vlan-id*]
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entries.	**show mac address-table aging-time**
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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

Removing Dynamic Address Entries

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

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

Configuring MAC Address Change Notification Traps

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

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

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	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.	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*
Step 3	Enable the switch module to send MAC address change notification traps to the NMS.	**snmp-server enable traps mac-notification change**
Step 4	Enable the MAC address change notification feature.	**mac address-table notification change**

	Step	Command
Step 5	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.	**mac address-table notification change** [**interval** *value*] [**history-size** *value*]
Step 6	Enter interface configuration mode, and specify the Layer 2 interface on which to enable the SNMP MAC address notification trap.	**interface** *interface-id*
Step 7	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.	**snmp trap mac-notification change** {**added** | **removed**}
Step 8	Return to privileged EXEC mode.	**end**
Step 9	Verify your entries.	**show mac address-table notification change interface** **show running-config**
Step 10	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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

This example shows how to specify 172.20.10.10 as the NMS, enable the switch module 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.

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

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	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.	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*
Step 3	Enable the switch module to send MAC address move notification traps to the NMS.	**snmp-server enable traps mac-notification move**
Step 4	Enable the MAC address move notification feature.	**mac address-table notification mac-move**
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify your entries.	**show mac address-table notification mac-move** **show running-config**
Step 7	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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

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

```
Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
```

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

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

Configuring MAC Threshold Notification Traps

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

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

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	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.	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*
Step 3	Enable the switch module to send MAC threshold notification traps to the NMS.	**snmp-server enable traps mac-notification threshold**
Step 4	Enable the MAC address threshold notification feature.	**mac address-table notification threshold**

	Step	Command
Step 5	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.	**mac address-table notification threshold** [**limit** *percentage*]	[**interval** *time*]
Step 6	Return to privileged EXEC mode.	**end**
Step 7	Verify your entries.	**show mac address-table notification threshold** **show running-config**
Step 8	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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

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

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

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

Adding and Removing Static Address Entries

A static address has these characteristics:

- It is manually entered in the address table and must be manually removed.
- It can be a unicast or multicast address.
- It does not age and is retained when the switch module 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 module 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 Chapter 12, "Private VLAN Configuration."

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

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

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

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

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

Configuring Unicast MAC Address Filtering

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

Follow these guidelines when using this feature:

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

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

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

- Packets that are forwarded to the CPU are also not supported.
- If you add a unicast MAC address as a static address and configure unicast MAC address filtering, the switch module 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 module 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 module adds the MAC address as a static address.

You enable unicast MAC address filtering and configure the switch module to drop packets with a specific address by specifying the source or destination unicast MAC address and the VLAN from which it is received.

Beginning in privileged EXEC mode, follow these steps to configure the switch module to drop a source or destination unicast static address:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enable unicast MAC address filtering and configure the switch module 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.	**mac address-table static** *mac-addr* **vlan** *vlan-id* **drop**
Step 3	Return to privileged EXEC mode.	**end**

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

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

This example shows how to enable unicast MAC address filtering and to configure the switch module 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 module. You can control MAC address learning on a VLAN to manage the available MAC address table space by controlling which VLANs, and which ports, can learn MAC addresses. Before you disable MAC address learning be sure that you are familiar with the network topology and the switch module system configuration. Disabling MAC address learning on a VLAN could cause flooding in the network.

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

- Use caution before disabling MAC address learning on a VLAN with a configured switch module virtual interface (SVI). The switch module 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 module is flooded in that VLAN domain.
- You cannot disable MAC address learning on a VLAN that is used internally by the switch module. If the VLAN ID that you enter is an internal VLAN, the switch module generates an error message and rejects the command. To view internal VLANs in use, enter the **show vlan internal usage** privileged EXEC command.
- If you disable MAC address learning on a VLAN configured as a private-VLAN primary VLAN, MAC addresses are still learned on the secondary VLAN that belongs to the private VLAN and are then replicated on the primary VLAN. If you disable MAC address learning on the secondary VLAN, but not the primary VLAN of a private VLAN, MAC address learning occurs on the primary VLAN and is replicated on the secondary VLAN.
- You cannot disable MAC address learning on an RSPAN VLAN. The configuration is not allowed.
- If you disable MAC address learning on a VLAN that includes a secure port, MAC address learning is not disabled on that port. If you disable port security, the configured MAC address learning state is enabled.

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

:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	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.	**no mac address-table learning vlan** *vlan-id*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify the configuration.	**show mac address-table learning** [**vlan** *vlan-id*]
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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 does not appear in the output from the **show running-config** command. The second command causes the configuration to appear in the **show running-config** privileged EXEC command display.

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

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

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

Displaying MAC Address Table Entries

You can display the MAC address table by using one or more of the privileged EXEC commands described in Table 6-6:

Table 6-6 Commands for Displaying the MAC Address Table

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.
show mac address-table dynamic	Displays only dynamic MAC address table entries.

Table 6-6 Commands for Displaying the MAC Address Table (continued)

Command	Description
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.

Managing the ARP Table

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

The Address Resolution Protocol (ARP) associates a host IP address with the corresponding media or MAC addresses and the VLAN ID. Using an IP address, ARP finds the associated MAC address. When a MAC address is found, the IP-MAC address association is stored in an ARP cache for rapid retrieval. Then the IP datagram is encapsulated in a link-layer frame and sent over the network. Encapsulation of IP datagrams and ARP requests and replies on 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 Chapter 2, “Command Line Interface” and the Cisco IOS Release 12.2 documentation on Cisco.com.

Switch Module Authentication

This chapter describes how to configure switch-based authentication on the CGR 2010 ESM, and contains the following topics:

Preventing Unauthorized Access to Your Switch Module

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

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

- At a minimum, you should configure passwords and privileges at each switch module port. These passwords are locally stored on the switch module. When users attempt to access the switch module through a port or line, they must enter the password specified for the port or line before they can access the switch module. For more information, see the "Protecting Access to Privileged EXEC Commands" section on page 7-2.
- For an additional layer of security, you can also configure username and password pairs, which are locally stored on the switch module. These pairs are assigned to lines or ports and authenticate each user before that user can access the switch module. If you have defined privilege levels, you can also assign a specific privilege level (with associated rights and privileges) to each username and password pair. For more information, see the "Configuring Username and Password Pairs" section on page 7-7.

- If you want to use username and password pairs, but you want to store them centrally on a server instead of locally, you can store them in a database on a security server. Multiple networking devices can then use the same database to obtain user authentication (and, if necessary, authorization) information. For more information, see the "Controlling Switch Module Access with TACACS+" section on page 7-11.

Protecting Access to Privileged EXEC Commands

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

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

Default Password and Privilege Level Configuration

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

Table 7-1 Default Password and Privilege Levels

Feature	Default Setting
Enable password and privilege level	No password is defined. The default is level 15 (privileged EXEC level). The password is not encrypted in the configuration file.
Enable secret password and privilege level	No password is defined. The default is level 15 (privileged EXEC level). The password is encrypted before it is written to the configuration file.
Line password	No password is defined

Setting or Changing a Static Enable Password

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

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

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

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

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

Protecting Enable and Enable Secret Passwords with Encryption

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

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

If you configure the **enable secret** command, it takes precedence over the **enable password** command; the two commands cannot be in effect simultaneously.

Beginning in privileged EXEC mode, follow these steps to configure encryption for enable and enable secret passwords:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Define a new password or change an existing password for access to privileged EXEC mode. or Define a secret password, which is saved using a nonreversible encryption method. • (Optional) For *level*, the range is from 0 to 15. Level 1 is normal user EXEC mode privileges. The default level is 15 (privileged EXEC mode privileges). • For *password*, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined. • (Optional) For *encryption-type*, only type 5, a Cisco proprietary encryption algorithm, is available. If you specify an encryption type, you must provide an encrypted password—an encrypted password that you copy from another switch module configuration. **Note** If you specify an encryption type and then enter a clear text password, you can not re-enter privileged EXEC mode. You cannot recover a lost encrypted password by any method.	**enable password** [**level** *level*] {*password* | *encryption-type encrypted-password*} or **enable secret** [**level** *level*] {*password* | *encryption-type encrypted-password*}
Step 3	(Optional) Encrypt the password when the password is defined or when the configuration is written. Encryption prevents the password from being readable in the configuration file.	**service password-encryption**

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

If both the enable and enable secret passwords are defined, users must enter the enable secret password.

Use the **level** keyword to define a password for a specific privilege level. After you specify the level and set a password, give the password only to users who need to have access at this level. Use the **privilege level** global configuration command to specify commands accessible at various levels. For more information, see the "Configuring Multiple Privilege Levels" section on page 7-8.

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

To remove a password and level, use the **no enable password** [**level** *level*] or **no enable secret** [**level** *level*] global configuration command. To disable password encryption, use the **no service password-encryption** global configuration command.

This example shows how to configure the encrypted password *1FaD0$Xyti5Rkls3LoyxzS8* for privilege level 2:

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

Disabling Password Recovery

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

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

Note If you disable password recovery, we recommend that you keep a backup copy of the configuration file on a secure server in case the end user interrupts the boot process and sets the system back to default values. Do not keep a backup copy of the configuration file on the switch module. We recommend that you also keep a backup copy of the VLAN database file on a secure server. When the switch module is returned to the default system configuration, you can download the saved files to the switch module by using the XMODEM protocol. For more information, see the "Recovering from a Lost or Forgotten Password" section on page 18-2.

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

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Disable password recovery. This setting is saved in an area of the flash memory that is accessible by the boot loader and the Cisco IOS image, but it is not part of the file system and is not accessible by any user.	**no service password-recovery**
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify the configuration by checking the last few lines of the command output.	**show version**

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

Note Disabling password recovery will not work if you have set the switch module to boot manually by using the **boot manual** global configuration command. This command produces the boot loader prompt (*switch:*) after the switch module is power cycled.

Setting a Telnet Password for a Terminal Line

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

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

	Step	Command
Step 1	Attach a PC or workstation with emulation software to the Cisco CGR 2010 router console port. The default data characteristics of the console port are 9600, 8, 1, no parity. You might need to press the Return key several times to see the command-line prompt.	
Step 2	Enter privileged EXEC mode.	**enable password** *password*
Step 3	Enter global configuration mode.	**configure terminal**
Step 4	Configure the number of Telnet sessions (lines), and enter line configuration mode. There are 16 possible sessions on a command-capable switch module. The 0 and 15 mean that you are configuring all 16 possible Telnet sessions.	**line vty 0 15**

	Step	Command
Step 5	Enter a Telnet password for the line or lines. For *password*, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined.	**password** *password*
Step 6	Return to privileged EXEC mode.	**end**
Step 7	Verify your entries. The password is listed under the command **line vty 0 15**.	**show running-config**
Step 8	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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

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

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

Configuring Username and Password Pairs

You can configure username and password pairs, which are locally stored on the switch module. These pairs are assigned to lines or ports and authenticate each user before that user can access the switch module. If you have defined privilege levels, you can also assign a specific privilege level (with associated rights and privileges) to each username and password pair.

Beginning in privileged EXEC mode, follow these steps to establish a username-based authentication system that requests a login username and a password:

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

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

Configuring Multiple Privilege Levels

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

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

These sections contain this configuration information:

- Setting the Privilege Level for a Command, page 7-9
- Changing the Default Privilege Level for Lines, page 7-10
- Logging into and Exiting a Privilege Level, page 7-11

Setting the Privilege Level for a Command

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

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

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

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

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

```
Switch(config)# privilege exec level 14 configure
Switch(config)# enable password level 14 SecretPswd14
```

Changing the Default Privilege Level for Lines

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

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Select the virtual terminal line on which to restrict access.	**line vty** *line*
Step 3	Change the default privilege level for the line. For *level*, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. Level 15 is the level of access permitted by the **enable** password.	**privilege level** *level*
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entries. The first command shows the password and access level configuration. The second command shows the privilege level configuration.	**show running-config** or **show privilege**
Step 6	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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

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

Logging into and Exiting a Privilege Level

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

	Step	Command
Step 1	Log in to a specified privilege level. For *level*, the range is 0 to 15.	**enable** *level*
Step 2	Exit to a specified privilege level. For *level*, the range is 0 to 15.	**disable** *level*

Controlling Switch Module Access with TACACS+

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

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

These sections contain this configuration information:

- Understanding TACACS+, page 7-11
- TACACS+ Operation, page 7-13
- Configuring TACACS+, page 7-13
- Displaying the TACACS+ Configuration, page 7-18

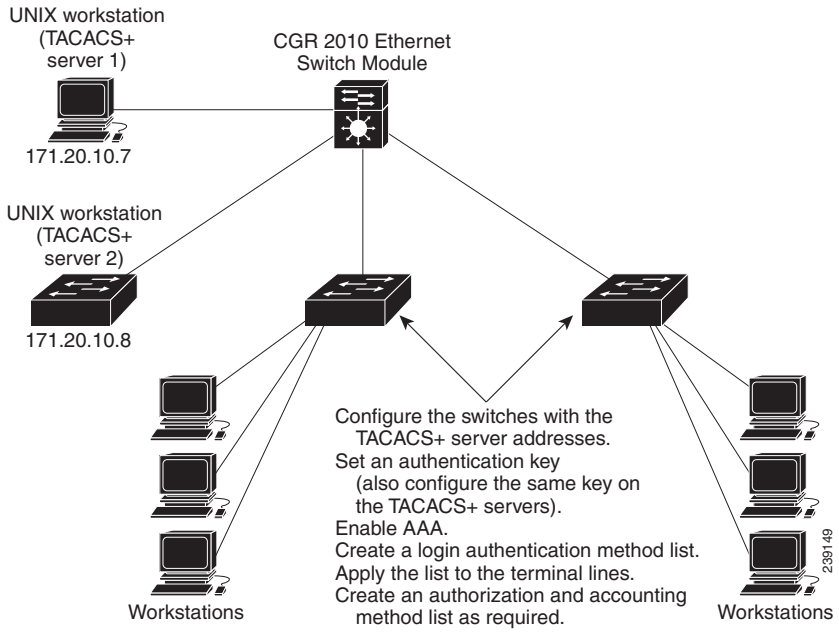
Understanding TACACS+

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

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

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

Figure 7-1 Typical TACACS+ Network Configuration



TACACS+, administered through the AAA security services, can provide these services:

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

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

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

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

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

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

TACACS+ Operation

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

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

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

2. The switch module eventually receives one of these responses from the TACACS+ daemon:

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

   After authentication, the user undergoes an additional authorization phase if authorization has been enabled on the switch module. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

3. If TACACS+ authorization is required, the TACACS+ daemon is again contacted, and it returns an ACCEPT or REJECT authorization response. If an ACCEPT response is returned, the response contains data in the form of attributes that direct the EXEC or NETWORK session for that user and the services that the user can access:

   - Telnet, Secure Shell (SSH), rlogin, or privileged EXEC services
   - Connection parameters, including the host or client IP address, access list, and user timeouts

Configuring TACACS+

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

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

For information about the command, see this URL:

http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/srfauth.html

These sections contain this configuration information:

Default TACACS+ Configuration

TACACS+ and AAA are disabled by default.

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

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

Identifying the TACACS+ Server Host and Setting the Authentication Key

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

Beginning in privileged EXEC mode, follow these steps to identify the IP host or host maintaining TACACS+ server and optionally set the encryption key:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Identify the IP host or hosts maintaining a TACACS+ server. Enter this command multiple times to create a list of preferred hosts. The software searches for hosts in the order in which you specify them. • For *hostname*, specify the name or IP address of the host. • (Optional) For **port** *integer*, specify a server port number. The default is port 49. The range is 1 to 65535. • (Optional) For **timeout** *integer*, specify a time in seconds the switch module waits for a response from the daemon before it times out and declares an error. The default is 5 seconds. The range is 1 to 1000 seconds. • (Optional) For **key** *string*, specify the encryption key for encrypting and decrypting all traffic between the switch module and the TACACS+ daemon. You must configure the same key on the TACACS+ daemon for encryption to be successful.	**tacacs-server host** *hostname* [**port** *integer*] [**timeout** *integer*] [**key** *string*]
Step 3	Enable AAA.	**aaa new-model**
Step 4	(Optional) Define the AAA server-group with a group name. This command puts the switch module in a server group subconfiguration mode.	**aaa group server tacacs+** *group-name*
Step 5	(Optional) Associate a particular TACACS+ server with the defined server group. Repeat this step for each TACACS+ server in the AAA server group. Each server in the group must be previously defined in Step 2.	**server** *ip-address*
Step 6	Return to privileged EXEC mode.	**end**
Step 7	Verify your entries.	**show tacacs**
Step 8	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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

Configuring TACACS+ Login Authentication

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

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

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

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enable AAA.	**aaa new-model**

To disable AAA, use the **no aaa new-model** global configuration command. To disable AAA authentication, use the **no aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] global configuration command. To either disable TACACS+ authentication for logins or to return to the default value, use the **no login authentication** {**default** | *list-name*} line configuration command.

Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services

AAA authorization limits the services available to a user. When AAA authorization is enabled, the switch module uses information retrieved from the user's profile, which is located either in the local user database or on the security server, to configure the user's session. The user is granted access to a requested service only if the information in the user profile allows it.

You can use the **aaa authorization** global configuration command with the **tacacs+** keyword to set parameters that restrict a user's network access to privileged EXEC mode.

The **aaa authorization exec tacacs+ local** command sets these authorization parameters:

- Use TACACS+ for privileged EXEC access authorization if authentication was performed by using TACACS+
- Use the local database if authentication was not performed by using TACACS+

Note Authorization is bypassed for authenticated users who log in through the CLI even if authorization has been configured.

Beginning in privileged EXEC mode, follow these steps to specify TACACS+ authorization for privileged EXEC access and network services:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Configure the switch module for user TACACS+ authorization for all network-related service requests.	**aaa authorization network tacacs+**
Step 3	Configure the switch module for user TACACS+ authorization if the user has privileged EXEC access. The **exec** keyword might return user profile information (such as **autocommand** information).	**aaa authorization exec tacacs+**
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entries.	**show running-config**
Step 6	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To disable authorization, use the **no aaa authorization** {**network** | **exec**} *method1* global configuration command.

Starting TACACS+ Accounting

The AAA accounting feature tracks the services that users are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the switch module reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, or auditing.

Beginning in privileged EXEC mode, follow these steps to enable TACACS+ accounting for each Cisco IOS privilege level and for network services:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enable TACACS+ accounting for all network-related service requests.	**aaa accounting network start-stop tacacs+**
Step 3	Enable TACACS+ accounting to send a start-record accounting notice at the beginning of a privileged EXEC process and a stop-record at the end.	**aaa accounting exec start-stop tacacs+**
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entries.	**show running-config**
Step 6	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To disable accounting, use the **no aaa accounting** {**network** | **exec**} {**start-stop**} *method1...* global configuration command.

Displaying the TACACS+ Configuration

To display TACACS+ server statistics, use the **show tacacs** privileged EXEC command.

Controlling Switch Module Access with RADIUS

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

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

These sections contain the following configuration information:

- Understanding RADIUS, page 7-18
- RADIUS Operation, page 7-19
- Configuring RADIUS, page 7-20
- Displaying the RADIUS Configuration, page 7-32

Understanding RADIUS

RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on supported Cisco routers and switches. Clients send authentication requests to a central RADIUS server, which contains all user authentication and network service access information.

The RADIUS host is normally a multiuser system running RADIUS server software from Cisco (Cisco Secure Access Control Server Version 3.0), Livingston, Merit, Microsoft, or another software provider. For more information, see the RADIUS server documentation.

Use RADIUS in these network environments that require access security:

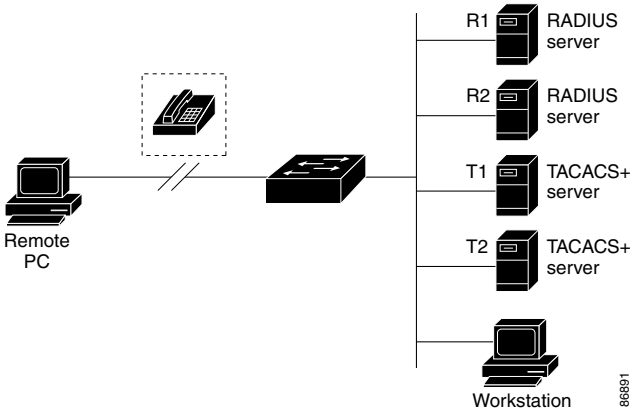
- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors' access servers, dial-in users are authenticated through a RADIUS server that has been customized to work with the Kerberos security system.
- Turnkey network security environments in which applications support the RADIUS protocol, such as in an access environment that uses a *smart card* access control system. In one case, RADIUS has been used with Enigma's security cards to validates users and to grant access to network resources.
- Networks already using RADIUS. You can add a Cisco switch containing a RADIUS client to the network. This might be the first step when you make a transition to a TACACS+ server. See Figure 7-2 on page 7-19.

- Network in which the user must only access a single service. Using RADIUS, you can control user access to a single host, to a single utility such as Telnet, or to the network through a protocol such as IEEE 802.1x. For more information about this protocol, see Chapter 10, "Configuring IEEE 802.1x Port-Based Authentication," in the *Cisco CGS 2520 Software Configuration Guide*.
- Networks that require resource accounting. You can use RADIUS accounting independently of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, showing the amount of resources (such as time, packets, bytes, and so forth) used during the session. An Internet service provider might use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.

RADIUS is not suitable in these network security situations:

- Multiprotocol access environments. RADIUS does not support AppleTalk Remote Access (ARA), NetBIOS Frame Control Protocol (NBFCP), NetWare Asynchronous Services Interface (NASI), or X.25 PAD connections.
- Switch-to-switch or router-to-router situations. RADIUS does not provide two-way authentication. RADIUS can be used to authenticate from one device to a non-Cisco device if the non-Cisco device requires authentication.
- Networks using a variety of services. RADIUS generally binds a user to one service model.

Figure 7-2 Transitioning from RADIUS to TACACS+ Services



RADIUS Operation

When a user attempts to log in and authenticate to a switch module that is access-controlled by a RADIUS server:

1. The user is prompted to enter a username and password.
2. The username and encrypted password are sent over the network to the RADIUS server.
3. The user receives one of these responses from the RADIUS server:
   a. ACCEPT—The user is authenticated.
   b. REJECT—The user is either not authenticated and is prompted to re-enter the username and password, or access is denied.
   c. CHALLENGE—A challenge requires additional data from the user.
   d. CHALLENGE PASSWORD—A response requests the user to select a new password.

The ACCEPT or REJECT response is bundled with additional data that is used for privileged EXEC or network authorization. Users must first successfully complete RADIUS authentication before proceeding to RADIUS authorization, if it is enabled. The additional data included with the ACCEPT or REJECT packets includes these items:

- Telnet, SSH, rlogin, or privileged EXEC services
- Connection parameters, including the host or client IP address, access list, and user timeouts.

Configuring RADIUS

This section describes how to configure your switch module to support RADIUS. At a minimum, you must identify the host or hosts that run the RADIUS server software and define the method lists for RADIUS authentication. You can optionally define method lists for RADIUS authorization and accounting.

A method list defines the sequence and methods to be used to authenticate, to authorize, or to keep accounts on a user. You can use method lists to designate one or more security protocols to be used (such as TACACS+ or local username lookup), ensuring a backup system if the initial method fails. The software uses the first method listed to authenticate, to authorize, or to keep accounts on users; if that method does not respond, the software selects the next method in the list. This process continues until there is successful communication with a listed method or the method list is exhausted.

You should have access to and should configure a RADIUS server before configuring RADIUS features on your switch module.

These sections contain this configuration information:

Default RADIUS Configuration

RADIUS and AAA are disabled by default.

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

Identifying the RADIUS Server Host

Switch-to-RADIUS-server communication involves several components:

- Hostname or IP address
- Authentication destination port
- Accounting destination port
- Key string
- Timeout period
- Retransmission value

You identify RADIUS security servers by their hostname or IP address, hostname and specific UDP port numbers, or their IP address and specific UDP port numbers. The combination of the IP address and the UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address.

If two different host entries on the same RADIUS server are configured for the same service—for example, accounting—the second host entry configured acts as a fail-over backup to the first one. Using this example, if the first host entry fails to provide accounting services, the switch module tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order that they are configured.)

A RADIUS server and the switch module use a shared secret text string to encrypt passwords and exchange responses. To configure RADIUS to use the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text (key) string that it shares with the switch module.

The timeout, retransmission, and encryption key values can be configured globally for all RADIUS servers, on a per-server basis, or in some combination of global and per-server settings. To apply these settings globally to all RADIUS servers communicating with the switch module, use the three unique global configuration commands: **radius-server timeout**, **radius-server retransmit**, and **radius-server key**. To apply these values on a specific RADIUS server, use the **radius-server host** global configuration command.

You can configure the switch module to use AAA server groups to group existing server hosts for authentication. For more information, see the "Defining AAA Server Groups" section on page 7-25.

Beginning in privileged EXEC mode, follow these steps to configure per-server RADIUS server communication. This procedure is required.

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enable AAA authentication.	**aaa new-model**

Step		Command
Step 3	Specify the IP address or hostname of the remote RADIUS server host. • (Optional) For **auth-port** *port-number*, specify the UDP destination port for authentication requests. • (Optional) For **acct-port** *port-number*, specify the UDP destination port for accounting requests. • (Optional) For **timeout** *seconds*, specify the time interval that the switch module waits for the RADIUS server to reply before resending. The range is 1 to 1000. This setting overrides the **radius-server timeout** global configuration command setting. If no timeout is set with the **radius-server host** command, the setting of the **radius-server timeout** command is used. • (Optional) For **retransmit** *retries*, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the **radius-server host** command, the setting of the **radius-server retransmit** global configuration command is used. • (Optional) For **key** *string*, specify the authentication and encryption key used between the switch module and the RADIUS daemon running on the RADIUS server. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. To configure the switch module to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. the switch module software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

	Step	Command
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entries.	**show running-config**
Step 6	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To remove the specified RADIUS server, use the **no radius-server host** *hostname* | *ip-address* global configuration command.

This example shows how to configure one RADIUS server to be used for authentication and another to be used for accounting:

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

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

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

Note You also need to configure some settings on the RADIUS server. These settings include the IP address of the switch module and the key string to be shared by both the server and the switch module. For more information, see the RADIUS server documentation.

Configuring RADIUS Login Authentication

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

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

Beginning in privileged EXEC mode, follow these steps to configure login authentication. This procedure is required.

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enable AAA.	**aaa new-model**

	Step	Command
Step 3	Create a login authentication method list. • To create a default list that is used when a named list is *not* specified in the **login authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all ports. • For *list-name*, specify a character string to name the list you are creating. • For *method1...*, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. Select one of these methods: – **enable**—Use the enable password for authentication. Before you can use this authentication method, you must define an enable password by using the **enable** *password* global configuration command. – **group radius**—Use RADIUS authentication. Before you can use this authentication method, you must configure the RADIUS server. For more information, see the "Identifying the RADIUS Server Host" section on page 7-21. – **line**—Use the line password for authentication. Before you can use this authentication method, you must define a line password. Use the **password** *password* line configuration command. – **local**—Use the local username database for authentication. You must enter username information in the database. Use the **username** *name* **password** global configuration command. – **local-case**—Use a case-sensitive local username database for authentication. You must enter username information in the database by using the **username** *password* global configuration command. – **none**—Do not use any authentication for login.	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]

	Step	Command
Step 4	Enter line configuration mode, and configure the lines to which you want to apply the authentication list.	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]
Step 5	Apply the authentication list to a line or set of lines. • If you specify **default**, use the default list created with the **aaa authentication login** command. • For *list-name*, specify the list created with the **aaa authentication login** command.	**login authentication** {**default** | *list-name*}
Step 6	Return to privileged EXEC mode.	**end**
Step 7	Verify your entries.	**show running-config**
Step 8	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To disable AAA, use the **no aaa new-model** global configuration command. To disable AAA authentication, use the **no aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] global configuration command. To either disable RADIUS authentication for logins or to return to the default value, use the **no login authentication** {**default** | *list-name*} line configuration command.

Defining AAA Server Groups

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

Server groups also can include multiple host entries for the same server if each entry has a unique identifier (the combination of the IP address and UDP port number), allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. If you configure two different host entries on the same RADIUS server for the same service, (for example, accounting), the second configured host entry acts as a fail-over backup to the first one.

You use the **server** group server configuration command to associate a particular server with a defined group server. You can either identify the server by its IP address or identify multiple host instances or entries by using the optional **auth-port** and **acct-port** keywords.

Beginning in privileged EXEC mode, follow these steps to define the AAA server group and associate a particular RADIUS server with it:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the IP address or hostname of the remote RADIUS server host. • (Optional) For **auth-port** *port-number*, specify the UDP destination port for authentication requests. • (Optional) For **acct-port** *port-number*, specify the UDP destination port for accounting requests. • (Optional) For **timeout** *seconds*, specify the time interval that the switch module waits for the RADIUS server to reply before resending. The range is 1 to 1000. This setting overrides the **radius-server timeout** global configuration command setting. If no timeout is set with the **radius-server host** command, the setting of the **radius-server timeout** command is used. • (Optional) For **retransmit** *retries*, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the **radius-server host** command, the setting of the **radius-server retransmit** global configuration command is used. • (Optional) For **key** *string*, specify the authentication and encryption key used between the switch module and the RADIUS daemon running on the RADIUS server. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. To configure the switch module to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The switch module software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]
Step 3	Enable AAA.	**aaa new-model**

	Step	Command
Step 4	Define the AAA server-group with a group name. This command puts the switch module in a server group configuration mode.	**aaa group server radius** *group-name*
Step 5	Associate a particular RADIUS server with the defined server group. Repeat this step for each RADIUS server in the AAA server group. Each server in the group must be previously defined in Step 2.	**server** *ip-address*
Step 6	Return to privileged EXEC mode.	**end**
Step 7	Verify your entries.	**show running-config**
Step 8	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**
Step 9	Enable RADIUS login authentication. See the "Configuring RADIUS Login Authentication" section on page 7-23.	

To remove the specified RADIUS server, use the **no radius-server host** *hostname* | *ip-address* global configuration command. To remove a server group from the configuration list, use the **no aaa group server radius** *group-name* global configuration command. To remove the IP address of a RADIUS server, use the **no server** *ip-address* server group configuration command.

In this example, the switch module is configured to recognize two different RADIUS group servers (*group1* and *group2*). Group1 has two different host entries on the same RADIUS server configured for the same services. The second host entry acts as a fail-over backup to the first entry.

```
Switch(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
Switch(config)# aaa new-model
Switch(config)# aaa group server radius group1
Switch(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config-sg-radius)# exit
Switch(config)# aaa group server radius group2
Switch(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
Switch(config-sg-radius)# exit
```

Configuring RADIUS Authorization for User Privileged Access and Network Services

AAA authorization limits the services available to a user. When AAA authorization is enabled, the switch module uses information retrieved from the user's profile, which is in the local user database or on the security server, to configure the user's session. The user is granted access to a requested service only if the information in the user profile allows it.

You can use the **aaa authorization** global configuration command with the **radius** keyword to set parameters that restrict a user's network access to privileged EXEC mode.

The **aaa authorization exec radius local** command sets these authorization parameters:

- Use RADIUS for privileged EXEC access authorization if authentication was performed by using RADIUS
- Use the local database if authentication was not performed by using RADIUS

Note Authorization is bypassed for authenticated users who log in through the CLI even if authorization has been configured.

Beginning in privileged EXEC mode, follow these steps to specify RADIUS authorization for privileged EXEC access and network services:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Configure the switch module for user RADIUS authorization for all network-related service requests.	**aaa authorization network radius**
Step 3	Configure the switch module for user RADIUS authorization if the user has privileged EXEC access. The **exec** keyword might return user profile information (such as **autocommand** information).	**aaa authorization exec radius**
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entries.	**show running-config**
Step 6	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To disable authorization, use the **no aaa authorization** {**network** | **exec**} *method1* global configuration command.

Starting RADIUS Accounting

The AAA accounting feature tracks the services that users are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the switch module reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, or auditing.

Beginning in privileged EXEC mode, follow these steps to enable RADIUS accounting for each Cisco IOS privilege level and for network services:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enable RADIUS accounting for all network-related service requests.	**aaa accounting network start-stop radius**
Step 3	Enable RADIUS accounting to send a start-record accounting notice at the beginning of a privileged EXEC process and a stop-record at the end.	**aaa accounting exec start-stop radius**
Step 4	Return to privileged EXEC mode.	**end**

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

To disable accounting, use the **no aaa accounting** {**network** | **exec**} {**start-stop**} *method1...* global configuration command.

Configuring Settings for All RADIUS Servers

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

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the shared secret text string used between the switch module and all RADIUS servers. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.	**radius-server key** *string*
Step 3	Specify the number of times the switch module sends each RADIUS request to the server before giving up. The default is 3; the range 1 to 1000.	**radius-server retransmit** *retries*
Step 4	Specify the number of seconds a switch module waits for a reply to a RADIUS request before resending the request. The default is 5 seconds; the range is 1 to 1000.	**radius-server timeout** *seconds*
Step 5	Specify the number of minutes a RADIUS server, which is not responding to authentication requests, to be skipped, avoiding the wait for the request to timeout before trying the next configured server. The default is 0; the range is 1 to 1440 minutes.	**radius-server deadtime** *minutes*
Step 6	Return to privileged EXEC mode.	**end**
Step 7	Verify your settings.	**show running-config**
Step 8	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To return to the default setting for the retransmit, timeout, and deadtime, use the **no** forms of these commands.

Configuring the Switch Module to Use Vendor-Specific RADIUS Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the switch module and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option by using the format recommended in the specification. Cisco's vendor-ID is 9, and the supported option has vendor-type 1, which is named *cisco-avpair*. The value is a string with this format:

```
protocol : attribute sep value *
```

Protocol is a value of the Cisco protocol attribute for a particular type of authorization. *Attribute* and *value* are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification, and *sep* is = for mandatory attributes and is * for optional attributes. The full set of features available for TACACS+ authorization can then be used for RADIUS.

For example, this AV pair activates Cisco's *multiple named ip address pools* feature during IP authorization (during PPP IPCP address assignment):

```
cisco-avpair= "ip:addr-pool=first"
```

This example shows how to provide a user logging in from a switch module with immediate access to privileged EXEC commands:

```
cisco-avpair= "shell:priv-lvl=15"
```

This example shows how to specify an authorized VLAN in the RADIUS server database:

```
cisco-avpair= "tunnel-type(#64)=VLAN(13)"
cisco-avpair= "tunnel-medium-type(#65)=802 media(6)"
cisco-avpair= "tunnel-private-group-ID(#81)=vlanid"
```

This example shows how to apply an input ACL in ASCII format to an interface for the duration of this connection:

```
cisco-avpair= "ip:inacl#1=deny ip 10.10.10.10 0.0.255.255 20.20.20.20 255.255.0.0"
cisco-avpair= "ip:inacl#2=deny ip 10.10.10.10 0.0.255.255 any"
cisco-avpair= "mac:inacl#3=deny any any decnet-iv"
```

This example shows how to apply an output ACL in ASCII format to an interface for the duration of this connection:

```
cisco-avpair= "ip:outacl#2=deny ip 10.10.10.10 0.0.255.255 any"
```

Other vendors have their own unique vendor-IDs, options, and associated VSAs. For more information about vendor-IDs and VSAs, see RFC 2138, "Remote Authentication Dial-In User Service (RADIUS)."

Beginning in privileged EXEC mode, follow these steps to configure the switch module to recognize and use VSAs:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enable the switch module to recognize and use VSAs as defined by RADIUS IETF attribute 26. • (Optional) Use the **accounting** keyword to limit the set of recognized vendor-specific attributes to only accounting attributes. • (Optional) Use the **authentication** keyword to limit the set of recognized vendor-specific attributes to only authentication attributes. If you enter this command without keywords, both accounting and authentication vendor-specific attributes are used.	**radius-server vsa send** [**accounting** | **authentication**]
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your settings.	**show running-config**
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

For a complete list of RADIUS attributes or more information about vendor-specific attribute 26, see the "RADIUS Attributes" appendix in the *Cisco IOS Security Configuration Guide, Release 12.2*.

Configuring the Switch Module for Vendor-Proprietary RADIUS Server Communication

Although an IETF draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the switch module and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. Cisco IOS software supports a subset of vendor-proprietary RADIUS attributes.

As mentioned earlier, to configure RADIUS (whether vendor-proprietary or IETF draft-compliant), you must specify the host running the RADIUS server daemon and the secret text string it shares with the switch module. You specify the RADIUS host and secret text string by using the **radius-server** global configuration commands.

Beginning in privileged EXEC mode, follow these steps to specify a vendor-proprietary RADIUS server host and a shared secret text string:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the IP address or hostname of the remote RADIUS server host and identify that it is using a vendor-proprietary implementation of RADIUS.	**radius-server host** {*hostname* | *ip-address*} **non-standard**

	Step	Command
Step 3	Specify the shared secret text string used between the switch module and the vendor-proprietary RADIUS server. the switch module and the RADIUS server use this text string to encrypt passwords and exchange responses. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.	**radius-server key** *string*
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your settings.	**show running-config**
Step 6	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To delete the vendor-proprietary RADIUS host, use the **no radius-server host** {*hostname* | *ip-address*} **non-standard** global configuration command. To disable the key, use the **no radius-server key** global configuration command.

This example shows how to specify a vendor-proprietary RADIUS host and to use a secret key of *rad124* between the switch module and the server:

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

Configuring RADIUS Server Load Balancing

This feature allows access and authentication requests to be evenly across all RADIUS servers in a server group. For more information, see the "RADIUS Server Load Balancing" chapter of the "Cisco IOS Security Configuration Guide", Release 12.2:

http://www.ciscosystems.com/en/US/docs/ios/12_2sb/feature/guide/sbrdldbl.html

Displaying the RADIUS Configuration

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

Controlling Switch Module Access with Kerberos

This section describes how to enable and configure the Kerberos security system, which authenticates requests for network resources by using a trusted third party. To use this feature, the cryptographic (that is, supports encryption) version of the switch module software must be installed on your switch module. You must obtain authorization to use this feature and to download the cryptographic software files from Cisco.com. For more information, see the release notes for this release.

These sections contain this information:

For Kerberos configuration examples, see the "Kerberos Configuration Examples" section in the "Security Server Protocols" chapter of the *Cisco IOS Security Configuration Guide, Release 12.2,* at this URL:

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfrad.html

For complete syntax and usage information for the commands used in this section, see the "Kerberos Commands" section in the "Security Server Protocols" chapter of the *Cisco IOS Security Command Reference, Release 12.2,* at this URL:

http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/fsecur_r.html

Note In the Kerberos configuration examples and in the *Cisco IOS Security Command Reference, Release 12.2,* the trusted third party can be a CGR 2010 ESM that supports Kerberos, that is configured as a network security server, and that can authenticate users by using the Kerberos protocol.

Understanding Kerberos

Kerberos is a secret-key network authentication protocol, which was developed at the Massachusetts Institute of Technology (MIT). It uses the Data Encryption Standard (DES) cryptographic algorithm for encryption and authentication and authenticates requests for network resources. Kerberos uses the concept of a trusted third party to perform secure verification of users and services. This trusted third party is called the *key distribution center* (KDC).

Kerberos verifies that users are who they claim to be and the network services that they use are what the services claim to be. To do this, a KDC or trusted Kerberos server issues tickets to users. These tickets, which have a limited lifespan, are stored in user credential caches. The Kerberos server uses the tickets instead of usernames and passwords to authenticate users and network services.

Note A Kerberos server can be a CGR 2010 ESM that is configured as a network security server and that can authenticate users by using the Kerberos protocol.

The Kerberos credential scheme uses a process called *single logon*. This process authenticates a user once and then allows secure authentication (without encrypting another password) wherever that user credential is accepted.

This software release supports Kerberos 5, which allows organizations that are already using Kerberos 5 to use the same Kerberos authentication database on the KDC that they are already using on their other network hosts (such as UNIX servers and PCs).

In this software release, Kerberos supports these network services:

- Telnet
- rlogin
- rsh (Remote Shell Protocol)

Table 7-2 lists the common Kerberos-related terms and definitions:

Table 7-2 Kerberos Terms

Term	Definition
Authentication	A process by which a user or service identifies itself to another service. For example, a client can authenticate to a switch module or a switch module can authenticate to another switch module.
Authorization	A means by which the switch module identifies what privileges the user has in a network or on the switch module and what actions the user can perform.
Credential	A general term that refers to authentication tickets, such as TGTs (ticket granting tickets) and service credentials. Kerberos credentials verify the identity of a user or service. If a network service decides to trust the Kerberos server that issued a ticket, it can be used in place of re-entering a username and password. Credentials have a default lifespan of eight hours.
Instance	An authorization level label for Kerberos principals. Most Kerberos principals are of the form *user@REALM* (for example, smith@EXAMPLE.COM). A Kerberos principal with a Kerberos instance has the form *user/instance@REALM* (for example, smith/admin@EXAMPLE.COM). The Kerberos instance can be used to specify the authorization level for the user if authentication is successful. The server of each network service might implement and enforce the authorization mappings of Kerberos instances but is not required to do so. **Note** The Kerberos principal and instance names *must* be in all lowercase characters. **Note** The Kerberos realm name *must* be in all uppercase characters.
KDC	Key distribution center that consists of a Kerberos server and database program that is running on a network host.
Kerberized	A term that describes applications and services that have been modified to support the Kerberos credential infrastructure.
Kerberos realm	A domain consisting of users, hosts, and network services that are registered to a Kerberos server. The Kerberos server is trusted to verify the identity of a user or network service to another user or network service. **Note** The Kerberos realm name *must* be in all uppercase characters.
Kerberos server	A daemon that is running on a network host. Users and network services register their identity with the Kerberos server. Network services query the Kerberos server to authenticate to other network services.

Table 7-2 Kerberos Terms (continued)

Term	Definition
KEYTAB	Key table. A password that a network service shares with the KDC. In Kerberos 5 and later Kerberos versions, the network service authenticates an encrypted service credential by using the KEYTAB to decrypt it. In Kerberos versions earlier than Kerberos 5, KEYTAB is referred to as SRVTAB (server table).
Principal	Also known as a Kerberos identity, this is who you are or what a service is according to the Kerberos server. **Note** The Kerberos principal name *must* be in all lowercase characters.
Service credential	A credential for a network service. When issued from the KDC, this credential is encrypted with the password shared by the network service and the KDC. The password is also shared with the user TGT.
SRVTAB	Server table. A password that a network service shares with the KDC. In Kerberos 5 or later Kerberos versions, SRVTAB is referred to as KEYTAB.
TGT	Ticket granting ticket that is a credential that the KDC issues to authenticated users. When users receive a TGT, they can authenticate to network services within the Kerberos realm represented by the KDC.

Kerberos Operation

A Kerberos server can be a CGR 2010 ESM that is configured as a network security server and that can authenticate remote users by using the Kerberos protocol. Although you can customize Kerberos in a number of ways, remote users attempting to access network services must pass through three layers of security before they can access network services.

To authenticate to network services by using a CGR 2010 ESM as a Kerberos server, remote users must follow these steps:

1. Authenticating to a Boundary Switch Module, page 7-35
2. Obtaining a TGT from a KDC, page 7-36
3. Authenticating to Network Services, page 7-36

Authenticating to a Boundary Switch Module

This section describes the first layer of security through which a remote user must pass. The user must first authenticate to the boundary switch module. The following process then occurs:

1. The user opens an un-Kerberized Telnet connection to the boundary switch module.
2. The switch module prompts the user for a username and password.
3. The switch module requests a TGT from the KDC for this user.
4. The KDC sends an encrypted TGT that includes the user identity to the switch module.
5. The switch module attempts to decrypt the TGT by using the password that the user entered.

- If the decryption is successful, the user is authenticated to the switch module.
- If the decryption is not successful, the user repeats Step 2 either by re-entering the username and password (noting if Caps Lock or Num Lock is on or off) or by entering a different username and password.

A remote user who initiates a un-Kerberized Telnet session and authenticates to a boundary switch module is inside the firewall, but the user must still authenticate directly to the KDC before getting access to the network services. The user must authenticate to the KDC because the TGT that the KDC issues is stored on the switch module and cannot be used for additional authentication until the user logs on to the switch module.

Obtaining a TGT from a KDC

This section describes the second layer of security through which a remote user must pass. The user must now authenticate to a KDC and obtain a TGT from the KDC to access network services.

For instructions about how to authenticate to a KDC, see the "Obtaining a TGT from a KDC" section in the "Security Server Protocols" chapter of the *Cisco IOS Security Configuration Guide, Release 12.2,* at this URL:

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfkerb.html

Authenticating to Network Services

This section describes the third layer of security through which a remote user must pass. The user with a TGT must now authenticate to the network services in a Kerberos realm.

For instructions about how to authenticate to a network service, see the "Authenticating to Network Services" section in the "Security Server Protocols" chapter of the *Cisco IOS Security Configuration Guide, Release 12.2,* at this URL:

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfkerb.html

Configuring Kerberos

So that remote users can authenticate to network services, you must configure the hosts and the KDC in the Kerberos realm to communicate and mutually authenticate users and network services. To do this, you must identify them to each other. You add entries for the hosts to the Kerberos database on the KDC and add KEYTAB files generated by the KDC to all hosts in the Kerberos realm. You also create entries for the users in the KDC database.

When you add or create entries for the hosts and users, follow these guidelines:

- The Kerberos principal name *must* be in all lowercase characters
- The Kerberos instance name *must* be in all lowercase characters
- The Kerberos realm name *must* be in all uppercase characters

Note A Kerberos server can be a CGR 2010 ESM that is configured as a network security server and that can authenticate users by using the Kerberos protocol.

To set up a Kerberos-authenticated server-client system, follow these steps:

- Configure the KDC by using Kerberos commands

- Configure the switch module to use the Kerberos protocol

For instructions, see the "Kerberos Configuration Task List" section in the "Security Server Protocols" chapter of the *Cisco IOS Security Configuration Guide, Release 12.2,* at this URL:

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfkerb.html

Configuring the Switch Module for Local Authentication and Authorization

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

Beginning in privileged EXEC mode, follow these steps to configure the switch module for local AAA:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enable AAA.	**aaa new-model**
Step 3	Set the login authentication to use the local username database. The **default** keyword applies the local user database authentication to all ports.	**aaa authentication login default local**
Step 4	Configure user AAA authorization, check the local database, and allow the user to run an EXEC shell.	**aaa authorization exec local**
Step 5	Configure user AAA authorization for all network-related service requests.	**aaa authorization network local**
Step 6	Enter the local database, and establish a username-based authentication system. Repeat this command for each user. • For *name*, specify the user ID as one word. Spaces and quotation marks are not allowed. • (Optional) For *level*, specify the privilege level the user has after gaining access. The range is 0 to 15. Level 15 gives privileged EXEC mode access. Level 0 gives user EXEC mode access. • For *encryption-type*, enter 0 to specify that an unencrypted password follows. Enter 7 to specify that a hidden password follows. • For *password*, specify the password the user must enter to gain access to the switch module. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the **username** command.	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}

	Step	Command
Step 7	Return to privileged EXEC mode.	**end**
Step 8	Verify your entries.	**show running-config**
Step 9	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To disable AAA, use the **no aaa new-model** global configuration command. To disable authorization, use the **no aaa authorization** {**network** | **exec**} *method1* global configuration command.

Configuring the Switch Module for Secure Shell

This section describes how to configure the Secure Shell (SSH) feature. To use this feature, you must install the cryptographic (encrypted) software image on your switch module. You must obtain authorization to use this feature and to download the cryptographic software files from Cisco.com. For more information, see the release notes for this release.

These sections contain this information:

- Understanding SSH, page 7-38
- Configuring SSH, page 7-39
- Displaying the SSH Configuration and Status, page 7-42

For SSH configuration examples, see the "SSH Configuration Examples" section in the "Configuring Secure Shell" chapter of the *Cisco IOS Security Configuration Guide, Cisco IOS Release 12.2*, at this URL:

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfssh.html#wp1001292

Note For complete syntax and usage information for the commands used in this section, see the command reference for this release and the command reference for Cisco IOS Release 12.2 at this URL: http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/fsecur_r.html

Understanding SSH

SSH is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2).

This section consists of these topics:

- SSH Servers, Integrated Clients, and Supported Versions, page 7-39
- Limitations, page 7-39

SSH Servers, Integrated Clients, and Supported Versions

The SSH feature has an SSH server and an SSH integrated client, which are applications that run on the switch module. You can use an SSH client to connect to a switch module running the SSH server. The SSH server works with the SSH client supported in this release and with non-Cisco SSH clients. The SSH client also works with the SSH server supported in this release and with non-Cisco SSH servers.

The switch module supports an SSHv1 or an SSHv2 server, and the switch module supports an SSHv1 client.

SSH supports the Data Encryption Standard (DES) encryption algorithm, the Triple DES (3DES) encryption algorithm, and password-based user authentication.

SSH also supports these user authentication methods:

- TACACS+ (for more information, see the "Controlling Switch Module Access with TACACS+" section on page 7-11)
- RADIUS (for more information, see the "Controlling Switch Module Access with RADIUS" section on page 7-18)
- Local authentication and authorization (for more information, see the "Configuring the Switch Module for Local Authentication and Authorization" section on page 7-37)

Note This software release does not support IP Security (IPSec).

Limitations

These limitations apply to SSH:

- The switch module supports Rivest, Shamir, and Adelman (RSA) authentication.
- SSH supports only the execution-shell application.
- The SSH server and the SSH client are supported only on DES (56-bit) and 3DES (168-bit) data encryption software.
- The switch module supports the Advanced Encryption Standard (AES) encryption algorithm with a 128-bit key, 192-bit key, or 256-bit key. However, symmetric cipher AES to encrypt the keys is not supported.

Configuring SSH

This section has this configuration information:

- Configuration Guidelines, page 7-39
- Setting Up the Switch Module to Run SSH, page 7-40 (required)
- Configuring the SSH Server, page 7-41 (required only if you are configuring the switch module as an SSH server)

Configuration Guidelines

Follow these guidelines when configuring the switch module as an SSH server or SSH client:

- An RSA key pair generated by a SSHv1 server can be used by an SSHv2 server, and the reverse.

- If you get CLI error messages after entering the **crypto key generate rsa** global configuration command, an RSA key pair has not been generated. Reconfigure the hostname and domain, and then enter the **crypto key generate rsa** command. For more information, see the "Setting Up the Switch Module to Run SSH" section on page 7-40.
- When generating the RSA key pair, the message `No host name specified` might appear. If it does, you must configure a hostname by using the **hostname** global configuration command.
- When generating the RSA key pair, the message `No domain specified` might appear. If it does, you must configure an IP domain name by using the **ip domain-name** global configuration command.
- When configuring the local authentication and authorization authentication method, make sure that AAA is disabled on the console.

Setting Up the Switch Module to Run SSH

Follow these steps to set up your switch module to run SSH:

1. Download the cryptographic software image from Cisco.com. This step is required. For more information, see the release notes for this release.
2. Configure a hostname and IP domain name for the switch module. Follow this procedure only if you are configuring the switch module as an SSH server.
3. Generate an RSA key pair for the switch module, which automatically enables SSH. Follow this procedure only if you are configuring the switch module as an SSH server.
4. Configure user authentication for local or remote access. This step is required. For more information, see the "Configuring the Switch Module for Local Authentication and Authorization" section on page 7-37.

Beginning in privileged EXEC mode, follow these steps to configure a hostname and an IP domain name and to generate an RSA key pair. This procedure is required if you are configuring the switch module as an SSH server.

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Configure a hostname for your switch module.	**hostname** *hostname*
Step 3	Configure a host domain for your switch module.	**ip domain-name** *domain_name*
Step 4	Enable the SSH server for local and remote authentication on the switch module and generate an RSA key pair. We recommend that a minimum modulus size of 1024 bits. When you generate RSA keys, you are prompted to enter a modulus length. A longer modulus length might be more secure, but it takes longer to generate and to use.	**crypto key generate rsa**
Step 5	Return to privileged EXEC mode.	**end**

	Step	Command
Step 6	Show the version and configuration information for your SSH server. Show the status of the SSH server on the switch module.	**show ip ssh** or **show ssh**
Step 7	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To delete the RSA key pair, use the **crypto key zeroize rsa** global configuration command. After the RSA key pair is deleted, the SSH server is automatically disabled.

Configuring the SSH Server

Beginning in privileged EXEC mode, follow these steps to configure the SSH server:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	(Optional) Configure the switch module to run SSH Version 1 or SSH Version 2. • **1**—Configure the switch module to run SSH Version 1. • **2**—Configure the switch module to run SSH Version 2. If you do not enter this command or do not specify a keyword, the SSH server selects the latest SSH version supported by the SSH client. For example, if the SSH client supports SSHv1 and SSHv2, the SSH server selects SSHv2.	**ip ssh version** [**1** | **2**]

	Step	Command
Step 3	Configure the SSH control parameters: • Specify the time-out value in seconds; the default is 120 seconds. The range is 0 to 120 seconds. This parameter applies to the SSH negotiation phase. After the connection is established, the switch module uses the default time-out values of the CLI-based sessions. • By default, up to five simultaneous, encrypted SSH connections for multiple CLI-based sessions over the network are available (session 0 to session 4). After the execution shell starts, the CLI-based session time-out value returns to the default of 10 minutes. • Specify the number of times that a client can re-authenticate to the server. The default is 3; the range is 0 to 5. Repeat this step when configuring both parameters.	**ip ssh** {**timeout** *seconds* | **authentication-retries** *number*}
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Show the version and configuration information for your SSH server. Show the status of the SSH server connections on the switch module.	**show ip ssh** or **show ssh**
Step 6	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To return to the default SSH control parameters, use the **no ip ssh** {**timeout** | **authentication-retries**} global configuration command.

Displaying the SSH Configuration and Status

To display the SSH server configuration and status, use one or more of the privileged EXEC commands in Table 7-3:

Table 7-3 Commands for Displaying the SSH Server Configuration and Status

Command	Description
show ip ssh	Shows the version and configuration information for the SSH server.
show ssh	Shows the status of the SSH server.

For more information about these commands, see the "Secure Shell Commands" section in the "Other Security Features" chapter of the *Cisco IOS Security Command Reference, Cisco IOS Release 12.2,* at this URL:

http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/srfpass.html

Configuring the Switch Module for Secure Copy Protocol

The Secure Copy Protocol (SCP) feature provides a secure and authenticated method for copying switch module configurations or switch module image files. SCP relies on Secure Shell (SSH), an application and a protocol that provides a secure replacement for the Berkeley r-tools.

For SSH to work, the switch module needs an RSA public/private key pair. This is the same with SCP, which relies on SSH for its secure transport.

Because SSH also relies on AAA authentication, and SCP relies further on AAA authorization, correct configuration is necessary.

- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the switch module
- Because SCP relies on SSH for its secure transport, the router must have an Rivest, Shamir, and Adelman (RSA) key pair

Note When using SCP, you cannot enter the password into the copy command. You must enter the password when prompted.

Information About Secure Copy

To configure the Secure Copy feature, you should understand these concepts.

- The behavior of SCP is similar to that of remote copy (rcp), which comes from the Berkeley r-tools suite, except that SCP relies on SSH for security. SCP also requires that authentication, authorization, and accounting (AAA) authorization be configured so the router can determine whether the user has the correct privilege level.
- A user who has appropriate authorization can use SCP to copy any file in the Cisco IOS File System (IFS) to and from a switch module by using the **copy** command. An authorized administrator can also do this from a workstation.

For more information on how to configure and verify SCP, see the "Secure Copy Protocol" chapter of the *Cisco IOS New Features, Cisco IOS Release 12.2T,* at this URL:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t2/feature/guide/ftscp.html

Interface Configuration

This chapter defines the types of interfaces on the CGR 2010 ESM and describes how to configure them, and contains the following topics:

Note For complete syntax and usage information for the commands used in this chapter, see the online *Cisco IOS Interface Command Reference, Release 12.2.*

Understanding Interface Types

This section describes the different types of interfaces supported by the switch module with references to chapters that contain more detailed information about configuring these interface types. The rest of the chapter describes configuration procedures for physical interface characteristics.

UNI, NNI, and ENI Port Types

The CGR 2010 ESM supports user-network interfaces (UNIs), network node interfaces (NNIs), and enhanced network interfaces (ENIs).

- UNIs are typically connected to a host, such as a PC or a Cisco IP phone.
- NNIs are typically connected to a router or to another switch or switch module
- ENIs have the same 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).

Note By default, upon startup, all ports on the switch module are enabled as NNIs. The default status for an NNI is administratively up to allow a service provider remote access to the switch module during initial configuration.

The default state for a UNI or ENI is administratively down to prevent unauthorized users from gaining access to other ports as you configure the switch module. Traffic is not switched between these ports, and all arriving traffic at UNIs or ENIs must leave on NNIs to prevent a user from gaining access to another user's private network. If it is appropriate for two or more UNIs or ENIs to exchange traffic within the switch module, the UNIs and ENIs can be assigned to a community VLAN. For instructions on how to configure community VLANs, see Chapter 11, "VLAN Configuration."

Note Even though the default state for a UNI or ENI is shutdown, entering the **default interface** *interface-id* command changes the port to the enabled state.

A port can be reconfigured from UNI to NNI or ENI and the reverse. When a port is reconfigured as another interface type, it inherits all the characteristics of that interface type. When you reconfigure a UNI or ENI to be an NNI, you must enable the port before it becomes active.

Changing the port type from UNI to ENI does not affect the administrative state of the port. If the UNI status is shut down, it remains shut down when reconfigured as an ENI; if the port is in a no shutdown state, it remains in the no shutdown state. At any time, all ports on the switch module are either UNI, NNI, or ENI.

Port-Based VLANs

A VLAN is a switched network that is logically segmented by function, team, or application, without regard to the physical location of the users. For more information about VLANs, see Chapter 11, "VLAN Configuration." Packets received on a port are forwarded only to ports that belong to the same VLAN as the receiving port. Network devices in different VLANs cannot communicate with one another without a Layer 3 device to route traffic between the VLANs.

VLAN partitions provide hard firewalls for traffic in the VLAN, and each VLAN has its own MAC address table. A VLAN comes into existence when a local port is associated with the VLAN ID or when a user creates te VLAN ID.

To isolate VLANs of different customers in a service-provider network, the switch module uses UNI-ENI VLANs. UNI-ENI VLANs isolate user network interfaces (UNIs) or enhanced network interfaces (ENIs) on the switch module from UNIs or ENIs that belong to other customer VLANs. There are two types of UNI-ENI VLANs:

- UNI-ENI isolated VLAN—This is the default VLAN state for all VLANs created on the switch module. Local switching does not occur among UNIs or ENIs on the switch module that belong to the same UNI-ENI isolated VLAN.
- UNI-ENI community VLAN—Local switching is allowed among UNIs and ENIs on the switch module that belong to the same UNI community VLAN. If UNIs or ENIs belong to the same customer, and you want to switch packets between the ports, you can configure the common VLAN as a UNI-ENI community VLAN.

Note Local switching takes place between ENIs and UNIs in the same community VLAN. Because you can enable spanning tree on ENIs, but not on UNIs, you should use caution when configuring ENIs and UNIs in the same community VLAN. UNIs are always in the forwarding state.

For more information about UNI VLANs, see the "UNI-ENI VLANs" section on page 11-5.

To configure VLANs, use the **vlan** *vlan-id* global configuration command to enter VLAN configuration mode. The VLAN configurations for VLAN IDs 1 to 1005 are saved in the VLAN database. Extended-range VLANs (VLAN IDs 1006 to 4094) are not added to the VLAN database. VLAN configuration is saved in the switch module running configuration, and you can save it in the switch module startup configuration file by entering the **copy running-config startup-config** privileged EXEC command.

Add ports to a VLAN by using the **switchport** interface configuration commands:

- Identify the interface
- For a trunk port, set trunk characteristics, and if desired, define the VLANs to which it can belong
- For an access port, set and define the VLAN to which it belongs
- For a tunnel port, set and define the VLAN ID for the customer-specific VLAN tag. See Chapter 13, "IEEE 802.1Q and Layer 2 Protocol Tunneling Configuration."

Switch Module Ports

Switch module ports are Layer 2 only interfaces associated with a physical port. Switch module ports belong to one or more VLANs. A switch module port can be an access port, a trunk port, a private-VLAN port, or a tunnel port. You can configure a port as an access port or trunk port. You configure a private VLAN port as a host or promiscuous port that belongs to a private-VLAN primary or secondary VLAN. (Only NNIs can be configured as promiscuous ports.) You must manually configure tunnel ports as part of an asymmetric link connected to an IEEE 802.1Q trunk port. Switch module ports are used for managing the physical interface and associated Layer 2 protocols and do not handle routing or bridging.

Configure switch module ports by using the **switchport** interface configuration commands. Use the **switchport** command with no keywords to put an interface that is in Layer 3 mode into Layer 2 mode.

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

For detailed information about configuring access port and trunk port characteristics, see Chapter 11, "VLAN Configuration."

For more information about tunnel ports, see Chapter 13, "IEEE 802.1Q and Layer 2 Protocol Tunneling Configuration."

Access Ports

An access port belongs to and carries the traffic of only one VLAN. Traffic is received and sent in native formats with no VLAN tagging. Traffic arriving on an access port is assumed to belong to the VLAN assigned to the port. If an access port receives an 802.1Q tagged packet, the packet is dropped, and the source address is not learned. 802.1x can also be used for VLAN assignment.

Two types of access ports are supported:

- Static access ports are manually assigned to a VLAN
- VLAN membership of dynamic access ports is learned through incoming packets. By default, a dynamic access port is a member of no VLAN, and forwarding to and from the port is enabled only when the VLAN membership of the port is discovered. UNIs begin forwarding packets as soon as they are enabled. Dynamic access ports on the switch module are assigned to a VLAN by a VLAN Membership Policy Server (VMPS). The VMPS can be a Catalyst 6500 series switch; the switch module cannot be a VMPS server. Dynamic access ports for VMPS are only supported on UNIs and ENIs.

Trunk Ports

An 802.1Q trunk port carries the traffic of multiple VLANs and by default is a member of all VLANs in the VLAN database. A trunk port supports simultaneous tagged and untagged traffic. An 802.1Q trunk port is assigned a default Port VLAN ID (PVID), and all untagged traffic travels on the port default PVID. All untagged traffic and tagged traffic with a NULL VLAN ID are assumed to belong to the port default PVID. A packet with a VLAN ID equal to the outgoing port default PVID is sent untagged. All other traffic is sent with a VLAN tag.

Although by default a trunk port is a member of multiple VLANs, you can limit VLAN membership by configuring an allowed list of VLANs for each trunk port. The list of allowed VLANs does not affect any other port but the associated trunk port. By default, all possible VLANs (VLAN ID 1 to 4094) are in the allowed list. A trunk port can become a member of a VLAN only if the VLAN is in the enabled state.

For more information about trunk ports, see Chapter 11, "VLAN Configuration."

Tunnel Ports

Tunnel ports are used in 802.1Q tunneling to segregate the traffic of customers in a service-provider network from other customers who are using the same VLAN number. You configure an asymmetric link from a tunnel port on a service-provider edge switch module to an 802.1Q trunk port on the customer switch module. Packets entering the tunnel port on the edge switch module, already IEEE 802.1Q-tagged with the customer VLANs, are encapsulated with another layer of an 802.1Q tag (called the metro tag), containing a VLAN ID unique in the service-provider network, for each customer. The double-tagged packets go through the service-provider network keeping the original customer VLANs separate from those of other customers. At the outbound interface, also a tunnel port, the metro tag is removed, and the original VLAN numbers from the customer network are retrieved.

Tunnel ports cannot be trunk ports or access ports and must belong to a VLAN unique to each customer.

For more information about tunnel ports, see Chapter 13, "IEEE 802.1Q and Layer 2 Protocol Tunneling Configuration."

Routed Ports

A routed port is a physical port that acts like a port on a router; it does not have to be connected to a router. A routed port is not associated with a particular VLAN, as is an access port. A routed port behaves like a regular router interface, except that it does not support VLAN subinterfaces. Routed ports can be configured with a Layer 3 routing protocol. A routed port is a Layer 3 interface only and does not support Layer 2 protocols, such as STP.

Configure routed ports by putting the interface into Layer 3 mode with the no switchport interface configuration command. Then assign an IP address to the port, enable routing, and assign routing protocol characteristics by using the ip routing and router protocol global configuration commands.

Configure routed ports by putting the interface into Layer 3 mode with the **no switchport** interface configuration command. Then assign an IP address to the port, enable routing, and assign routing protocol characteristics by using the **ip routing** and **router** *protocol* global configuration commands.

Note Entering a **no switchport** interface configuration command shuts down the interface and then re-enables it, which might generate messages on the device to which the interface is connected. When you put an interface that is in Layer 2 mode into Layer 3 mode, the previous configuration information related to the affected interface might be lost.

The number of routed ports that you can configure is not limited by software. However, the interrelationship between this number and the number of other features being configured might impact CPU performance because of hardware limitations. See the "Configuring Layer 3 Interfaces" section on page 8-34 for information about what happens when hardware resource limitations are reached.

For more information about IP unicast and multicast routing and routing protocols, see:

- Chapter 18, "Configuring IP Unicast Routing" in the *Cisco CGS 2520 Switch Software Configuration Guide*

  http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swiprout.html

  Chapter 19, "Configuring IPv6 Unicast Routing" in the *Cisco CGS 2520 Switch Software Configuration Guide*

  http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swipv6.html

Note For full Layer 3 routing, you must have the IP services image installed on the switch module.

Switch Virtual Interfaces

A Switch Virtual Interface (SVI) represents a VLAN of switch module ports as one interface to the routing or bridging function in the system. Only one SVI can be associated with a VLAN, but you need to configure an SVI for a VLAN only when you wish to route between VLANs or to provide IP host connectivity to the switch module. By default, an SVI is created for the default VLAN (VLAN 1) to permit remote switch administration. Additional SVIs must be explicitly configured.

Note You cannot delete interface VLAN 1.

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

Although the switch module supports a total of 1,005 VLANs (and SVIs), the interrelationship between the number of SVIs and routed ports and the number of other features being configured might impact CPU performance because of hardware limitations. See the "Configuring Layer 3 Interfaces" section on page 8-34 for information about what happens when hardware resource limitations are reached.

SVIs are created the first time that you enter the **vlan** interface configuration command for a VLAN interface. The VLAN corresponds to the VLAN tag associated with data frames on an IEEE 802.1Q encapsulated trunk or the VLAN ID configured for an access port. Configure a VLAN interface for each VLAN for which you want to route traffic, and assign it an IP address. For more information, see the "Manually Assigning IP Information" section on page 4-15.

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

- SVIs support routing protocols
- Routed ports (or SVIs) are supported only when the IP services image is installed on the switch module

EtherChannel Port Groups

EtherChannel port groups treat multiple switch module ports as one switch module port. These port groups act as a single logical port for high-bandwidth connections between switches or between switches and servers. An EtherChannel balances the traffic load across the links in the channel. If a link within the EtherChannel fails, traffic previously carried over the failed link changes to the remaining links.

You can group multiple trunk ports into one logical trunk port, group multiple access ports into one logical access port, group multiple tunnel ports into one logical tunnel port, or group multiple routed ports into one logical routed port. Most protocols operate over either single ports or aggregated switch module ports and do not recognize the physical ports within the port group. Exceptions are the Cisco Discovery Protocol (CDP), and Link Aggregation Control Protocol (LACP), which operate only on physical NNI or ENI ports.

When you configure an EtherChannel, you create a port-channel logical interface and assign an interface to the EtherChannel.

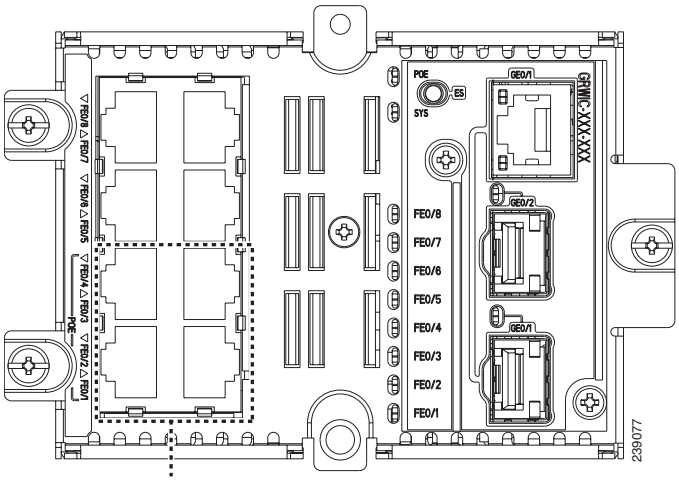
- For Layer 3 interfaces, you manually create the logical interface by using the **interface port-channel** global configuration command. Then you manually assign an interface to the EtherChannel by using the **channel-group** interface configuration command.
- For Layer 2 interfaces, use the **channel-group** interface configuration command to dynamically create the port-channel logical interface. This command binds the physical and logical ports together. For more information, see Chapter 15, "EtherChannel Configuration and Link State Tracking."

Power Over Ethernet Ports

There are four PoE-capable ports in the Copper model of the switch module: FE0/1, FE0/2, FE0/3, and FE0/4 (the lower four Fast Ethernet ports as shown in Figure 8-1).

Note Power over Ethernet (PoE) is supported only on the copper model.

Figure 8-1 Power Over Ethernet-Capable Ports in the Copper Model



The total PoE power budget for the Cisco CGR 2010 router is 61.6 watts, regardless of whether there are one or two Copper Ethernet switchs installed in the router. By default, the maximum PoE power per PoE-capable port is 15.4 watts. However, you can use the **power inline port max** command to set the maximum PoE power per PoE-capable port to a maximum of 20 watts.

To see what the power usage is for each of the PoE-capable ports, use the **show power inline** command.

PoE-capable switch module ports automatically supply power to these connected devices (if the switch module senses that there is no power on the circuit):

- Cisco pre-standard powered devices (such as Cisco IP Phones and Cisco Aironet access points)
- 802.3af-compliant powered devices

A powered device can receive redundant power when it is connected only to a PoE switch module port and to an AC power source.

After the switch module detects a powered device, it determines the device power requirements and then grants or denies power to the device. The switch module can also sense the real-time power consumption of the device by monitoring and policing the power usage.

This section provides the following PoE information:

- Supported Protocols and Standards, page 8-8
- Powered-Device Detection and Initial Power Allocation, page 8-8
- Power Management Modes, page 8-9

Supported Protocols and Standards

The switch module uses these protocols and standards to support PoE:

- Cisco Discovery Protocol (CDP) with power consumption—The powered device notifies the switch module of the amount of power it is consuming. The switch module does not reply to the power-consumption messages. The switch module can only supply power to or remove power from the PoE port.
- Cisco intelligent power management—The powered device and the switch module negotiate through power-negotiation CDP messages for an agreed power-consumption level. The negotiation allows a high-power Cisco powered device, which consumes more than 7 W, to operate at its highest power mode. The powered device first boots up in low-power mode, consumes less than 7 W, and negotiates to obtain enough power to operate in high-power mode. The device changes to high-power mode only when it receives confirmation from the switch module.

  High-power devices can operate in low-power mode on switches that do not support power-negotiation CDP.

  Cisco intelligent power management is backward-compatible with CDP with power consumption; the switch module responds according to the CDP message that it receives. CDP is not supported on third-party powered devices; the switch module uses the IEEE classification to determine the power usage of the device.
- IEEE 802.3af—The major features of this standard are powered-device discovery, power administration, disconnect detection, and optional powered-device power classification. For more information, see the standard.

Powered-Device Detection and Initial Power Allocation

The switch module detects a Cisco pre-standard or an IEEE-compliant powered device when the PoE-capable port is in the no-shutdown state, PoE is enabled (the default), and the connected device is not being powered by an AC adaptor.

After device detection, the switch module determines the device power requirements based on its type:

- A Cisco pre-standard powered device does not provide its power requirement when the switch module detects it, so the switch module allocates 15.4 W as the initial allocation for power budgeting.

  The initial power allocation is the maximum amount of power that a powered device requires. The switch module initially allocates this amount of power when it detects and powers the powered device. As the switch module receives CDP messages from the powered device and as the powered device negotiates power levels with the switch module through CDP power-negotiation messages, the initial power allocation might be adjusted.
- The switch module classifies the detected IEEE device within a power consumption class. Based on the available power in the power budget, the switch module determines if a port can be powered. Table 8-1 lists these power classification levels.

Table 8-1 IEEE Power Classifications

Class	Maximum Power Level Required from the Switch Module
0 (class status unknown)	15.4 W
1	4 W
2	7 W

Table 8-1 IEEE Power Classifications (continued)

Class	Maximum Power Level Required from the Switch Module
3	15.4 W
4 (reserved for future use)	treat as class 0

The switch module monitors and tracks requests for power and grants power only when it is available. The switch module tracks its power budget (the amount of power available on the switch module for PoE). The host CGR 2010 router performs power-accounting calculations and the switch module grants or denies power based on those calculations to keep the power budget up to date.

After power is applied to the port, the switch module uses CDP to determine the actual power consumption requirement of the connected Cisco powered devices, and the switch module adjusts the power budget accordingly. This does not apply to third-party PoE devices. The switch module processes a request and either grants or denies power. If the request is granted, the switch module updates the power budget. If the request is denied, the switch module ensures that power to the port is turned off, generates a syslog message, and updates the LEDs. Powered devices can also negotiate with the switch module for more power.

If the switch module detects a fault caused by an undervoltage, overvoltage, overtemperature, oscillator-fault, or short-circuit condition, it turns off power to the port, generates a syslog message, and updates the power budget and LEDs.

Power Management Modes

The switch module supports these PoE modes:

- **Auto**—The switch module automatically detects if the connected device requires power. If the switch module discovers a powered device connected to the port and if the switch module has enough power, it grants power, updates the power budget, turns on power to the port on a first-come, first-served basis, and updates the LEDs. For LED information, see the *Cisco Connected Grid 10-Port Ethernet Switch Module Interface Card Getting Started Guide*.

  If the switch module has enough power for all the powered devices, they all come up. If enough power is available for all powered devices connected to the switch module, power is turned on to all devices. If there is not enough available PoE, or if a device is disconnected and reconnected while other devices are waiting for power, it cannot be determined which devices are granted or are denied power.

  If granting power would exceed the system power budget, the switch module denies power, ensures that power to the port is turned off, generates a syslog message, and updates the LEDs. After power has been denied, the switch module periodically rechecks the power budget and continues to attempt to grant the request for power.

  If a device being powered by the switch module is then connected to wall power, the switch module might continue to power the device. The switch module might continue to report that it is still powering the device whether the device is being powered by the switch module or receiving power from an AC power source.

  If a powered device is removed, the switch module automatically detects the disconnect and removes power from the port. You can connect a nonpowered device without damaging it.

  You can specify the maximum wattage that is allowed on the port. If the IEEE class maximum wattage of the powered device is greater than the configured maximum value, the switch module does not provide power to the port. If the switch module powers a powered device, but the powered

device later requests through CDP messages more than the configured maximum value, the switch module removes power to the port. The power that was allocated to the powered device is reclaimed into the global power budget. If you do not specify a wattage, the switch module delivers the maximum value. Use the auto setting on any PoE port. The auto mode is the default setting.

- **Static**—The switch module pre-allocates power to the port (even when no powered device is connected) and guarantees that power will be available for the port. The switch module allocates the port configured maximum wattage, and the amount is never adjusted through the IEEE class or by CDP messages from the powered device. Because power is pre-allocated, any powered device that uses less than or equal to the maximum wattage is guaranteed to be powered when it is connected to the static port. The port no longer participates in the first-come, first-served model.

  However, if the powered-device IEEE class is greater than the maximum wattage, the switch module does not supply power to it. If the switch module learns through CDP messages that the powered device needs more than the maximum wattage, the powered device is shutdown.

  If you do not specify a wattage, the switch module pre-allocates the maximum value. The switch module powers the port only if it discovers a powered device. Use the static setting on a high-priority interface.

- **Never**—The switch module disables powered-device detection and never powers the PoE port even if an unpowered device is connected. Use this mode only when you want to make sure power is never applied to a PoE-capable port, making the port a data-only port.

For information on configuring a PoE-enabled port, see the "Configuring a Power Management Mode on a PoE-Enabled Port" section on page 8-25.

Power Monitoring and Power Policing

When policing of the real-time power consumption is enabled, the switch module takes action when a powered device consumes more power than the maximum amount allocated, also referred to as the *cutoff-power value*.

When PoE is enabled, the switch module senses the real-time power consumption of the powered device. The switch module monitors the real-time power consumption of the connected powered device; this is called *power monitoring* or *power sensing*. The switch module also polices the power usage with the *power policing* feature.

Power monitoring is backward-compatible with Cisco intelligent power management and CDP-based power consumption. It works with these features to ensure that the PoE port can supply power to the powered device. For more information about these PoE features, see the "Supported Protocols and Standards" section on page 8-8.

The switch module senses the real-time power consumption of the connected device as follows:

1. The switch module monitors the real-time power consumption on individual ports.
2. The switch module records the power consumption, including peak power usage. The switch module reports the information through the CISCO-POWER-ETHERNET-EXT-MIB.
3. If power policing is enabled, the switch module polices power usage by comparing the real-time power consumption to the maximum power allocated to the device. For more information about the maximum power consumption, also referred to as the cutoff power, on a PoE port, see the next section, "Maximum Power Allocation (Cutoff Power) on a PoE Port."

- If the device uses more than the maximum power allocation on the port, the switch module can either turn off power to the port, or the switch module can generate a syslog message and update the LEDs (the port LED is now blinking amber) while still providing power to the device based on the switch module configuration. By default, power-usage policing is disabled on all PoE ports.
- If error recovery from the PoE error-disabled state is enabled, the switch module automatically takes the PoE port out of the error-disabled state after the specified amount of time.
- If error recovery is disabled, you can manually re-enable the PoE port by using the **shutdown** and **no shutdown** interface configuration commands.

4. If policing is disabled, no action occurs when the powered device consumes more than the maximum power allocation on the PoE port, which could adversely affect the switch module.

Maximum Power Allocation (Cutoff Power) on a PoE Port

When power policing is enabled, the switch module determines one of the these values as the cutoff power on the PoE port in this order:

1. Manually when you set the user-defined power level that the switch module budgets for the port by using the **power inline consumption default** *wattage* global or interface configuration command.
2. Manually when you set the user-defined power level that limits the power allowed on the port by using the **power inline auto max** *max-wattage* or the **power inline static max** *max-wattage* interface configuration command.
3. Automatically when the switch module sets the power usage of the device by using CDP power negotiation or by the IEEE classification.
4. Automatically when the switch module sets the power usage to be the default value of 15400 mW.

To manually configure the cutoff-power value, use the first or second method in the previous list by entering the **power inline consumption default** *wattage* command or the **power inline [auto | static max]** *max-wattage* command.

If you are not manually configuring the cutoff-power value, the switch module automatically determines the value by using CDP power negotiation or the device IEEE classification, which is the third method in the previous list. If the switch module cannot determine the value by using one of these methods, it uses the default value of 15400 mW (the fourth method in the previous list).

Power Consumption Values

You can configure the initial power allocation and the maximum power allocation on a port. However, these values are only the configured values that determine when the switch module should turn on or turn off power on the PoE port. The maximum power allocation is not the same as the actual power consumption of the powered device. The actual cutoff power value that the switch module uses for power policing is not equal to the configured power value.

When power policing is enabled, the switch module polices the power usage at the switch module port, which is greater than the power consumption of the device. When you are manually set the maximum power allocation, you must consider the power loss over the cable from the switch module port to the powered device. The cutoff power is the sum of the rated power consumption of the powered device and the worst-case power loss over the cable.

The actual amount of power consumed by a powered device on a PoE port is the cutoff-power value plus a calibration factor of 500 mW (0.5 W). The actual cutoff value is approximate and varies from the configured value by a percentage of the configured value. For example, if the configured cutoff power is 12 W, the actual cutoff-value is 11.4 W, which is 5% less than the configured value.

We recommend that you enable power policing when PoE is enabled on your switch module. For example, if policing is disabled and you set the cutoff-power value by using the **power inline auto max 6300** interface configuration command, the configured maximum power allocation on the PoE port is 6.3 W (6300 mW).

The switch module provides power to the connected devices on the port if the device needs up to 6.3 W. If the CDP-power negotiated value or the IEEE classification value exceeds the configured cutoff value, the switch module does not provide power to the connected device. After the switch module turns on power on the PoE port, the switch module does not police the real-time power consumption of the device, and the device can consume more power than the maximum allocated amount, which could adversely affect the switch module and the devices connected to the other PoE ports.

Dual-Purpose Ports

The Gigabit Ethernet port GE0/1 on the switch module consists of a pair of one RJ-45 connector (topmost port) and one SFP module connector (bottom port).

This dual-purpose port is considered as a single interface. The two connectors are not redundant interfaces—the switch module activates only one connector of the pair at a time.

If the dual-purpose port is configured as **media-type RJ-45**, the speed of the connection can be manually set to either 10, 100 or 1000 MBPS (10/100/1000Base-T specifications). The default speed setting is always enabled to AUTONEGOTIATION. It will automatically negotiate to whatever speed is set on the other end of the connection.

If the dual-purpose port is configured as **media-type SFP,** the speed is dependent on the module type you are using, either a 100FX or a 1000Base-X SFP module. The port will automatically detect the module, and the speed is set based on the media type. The other end of the connection will have to be of the same media type to establish the link.

Note Even when operating at 100 Mbps, the dual-purpose ports (and the SFP-only module ports) use the frame size that is set with the **system mtu jumbo** global configuration command.

By default, the dual-purpose ports and the SFP-only module ports are network node interfaces (NNIs). The switch module dynamically selects the dual-purpose port media type that first links up. However, you can use the **media-type** interface configuration command to manually select the RJ-45 connector or the SFP-module connector. For information about configuring a dual-purpose port, see the "Configuring a Dual-Purpose Port" section on page 8-29.

Note In **auto-select** mode, if both copper and fiber-optic signals are simultaneously detected, the switch module gives preference to SFP mode.

Each dual-purpose port has two LEDs:

- One shows the status of the SFP module port
- One shows the status of the RJ-45 port

The port LED is on for whichever connector is active. For more information about the LEDs, see the *Cisco Connected Grid 10-Port Ethernet Switch Module Interface Card Getting Started Guide*.

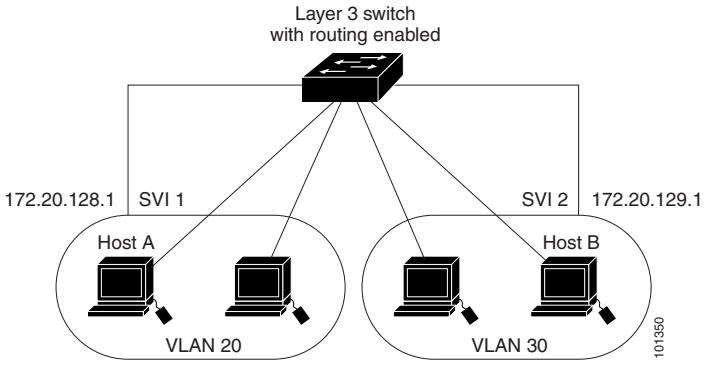
Connecting Interfaces

Devices within a single VLAN can communicate directly through any switch module. Ports in different VLANs cannot exchange data without going through a routing device. With a standard Layer 2 switch module, ports in different VLANs have to exchange information through a router.

By default, the CGR 2010 ESM provides VLAN isolation between UNIs or ENIs. UNIs and ENIs cannot exchange traffic unless they are changed to NNIs or assigned to a UNI-ENI community VLAN.

By using the switch module with routing enabled, when you configure both VLAN 20 and VLAN 30 with an SVI to which an IP address is assigned, packets can be sent from Host A to Host B directly through the switch module with no need for an external router (see Figure 8-2).

Figure 8-2 Connecting VLANs with the Switch Module



When the IP services image is running on the switch module, routing can be enabled on the switch module. Whenever possible, to maintain high performance, forwarding is done by the switch module hardware. However, only IP Version 4 packets with Ethernet II encapsulation can be routed in hardware. The routing function can be enabled on all SVIs and routed ports. The switch module routes only IP traffic. When IP routing protocol parameters and address configuration are added to an SVI or routed port, any IP traffic received from these ports is routed.

Using Interface Configuration Mode

The switch module supports these interface types:

- Physical ports—switch module ports, routed ports, UNIs, NNIs, and ENIs
- VLANs—switch module virtual interfaces
- Port-channels—EtherChannel interfaces

You can also configure a range of interfaces (see the "Configuring a Range of Interfaces" section on page 8-15).

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

- **Type**—Fast Ethernet (fastethernet or fa) for 10/100 Mbps Ethernet, Gigabit Ethernet (gigabitethernet or gi) for 10/100/1000 Mbps Ethernet ports, or small form-factor pluggable (SFP) module Gigabit Ethernet interfaces.
- **Module number**—The module or slot number on the switch module (always 0 on the CGR 2010 ESM).

- **Port number**—The interface number on the switch module. The port numbers always begin at 1, starting with the bottom rightmost port when facing the front of the switch module, for example, fastethernet 0/1 or gigabitethernet 0/1. If there is more than one interface type (for example, 10/100 ports and SFP module ports), the port numbers restart with the second interface type: GigabitEthernet 0/0/0 or 0/2/0.

You can identify physical interfaces by physically checking the interface location on the switch module. You can also use the **show** privileged EXEC commands to display information about a specific interface or all the interfaces on the switch module. The remainder of this chapter primarily provides physical interface configuration procedures.

Procedures for Configuring Interfaces

These general instructions apply to all interface configuration processes.

Step 1 Enter the **configure terminal** command at the privileged EXEC prompt:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

Step 2 Enter the **interface** global configuration command. Identify the interface type and the number of the connector. In this example, Fast Ethernet port 1 is selected:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)#
```

Note You do not need to add a space between the interface type and interface number. For example, in the preceding line, you can specify either **fastethernet 0/1**, **fastethernet0/1**, **fa 0/1**, or **fa0/1**.

Step 3 If you are configuring a UNI or ENI, enter the **no shutdown** interface configuration command to enable the interface:

```
Switch(config-if)# no shutdown
```

Step 4 Follow each **interface** command with the interface configuration commands that the interface requires. The commands that you enter define the protocols and applications that will run on the interface. The commands are collected and applied to the interface when you enter another interface command or enter **end** to return to privileged EXEC mode.

You can also configure a range of interfaces by using the **interface range** or **interface range macro** global configuration commands. Interfaces configured in a range must be the same type and must be configured with the same feature options.

Step 5 After you configure an interface, verify its status by using the **show** privileged EXEC commands listed in the "Monitoring and Maintaining the Interfaces" section on page 8-38.

Enter the **show interfaces** privileged EXEC command to see a list of all interfaces on or configured for the switch module. A report is provided for each interface that the device supports or for the specified interface.

Configuring a Range of Interfaces

You can use the **interface range** global configuration command to configure multiple interfaces with the same configuration parameters. When you enter the interface range configuration mode, all command parameters that you enter are attributed to all interfaces within that range until you exit this mode.

Beginning in privileged EXEC mode, follow these steps to configure a range of interfaces with the same parameters:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the range of interfaces (VLANs or physical ports) to be configured, and enter interface range configuration mode. • You can use the **interface range** command to configure up to five port ranges or a previously defined macro. • In a comma-separated *port-range*, you must enter the interface type for each entry and enter spaces before and after the comma. • In a hyphen-separated *port-range*, you do not need to re-enter the interface type, but you must enter a space before the hyphen.	**interface range** {*port-range*}
Step 3	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.	**no shutdown**
Step 4	Use the normal configuration commands to apply the configuration parameters to all interfaces in the range.	
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify the configuration of the interfaces in the range.	**show interfaces** [*interface-id*]
Step 7	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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

- Valid entries for *port-range*:
  - **vlan** *vlan-ID - vlan-ID*, where the VLAN ID is 1 to 4094
  - **fastethernet** module/{first *port*} - {*last port*}, where the module is always 0
  - **gigabitethernet** module/{*first port*} - {*last port*}, where the module is always 0
  - **port-channel** *port-channel-number - port-channel-number*, where the *port-channel-number* is 1 to 48

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

- The **interface range** command only works with VLAN interfaces that have been configured with the **interface vlan** command. The **show running-config** privileged EXEC command displays the configured VLAN interfaces. VLAN interfaces not displayed by the **show running-config** command cannot be used with the **interface range** command.
- All interfaces defined as in a range must be the same type (all Fast Ethernet ports, all Gigabit Ethernet ports, all EtherChannel ports, or all VLANs), but you can enter multiple ranges in a command.

This example shows how to use the **interface range** global configuration command to set the speed on ports 1 and 2 to 100 Mbps:

```
Switch# configure terminal
Switch(config)# interface range fastethernet0/1 - 2
Switch(config-if-range)# no shutdown
Switch(config-if-range)# speed 100
```

This example shows how to use a comma to add different interface type strings to the range to enable Fast Ethernet ports 1 to 3 and Gigabit Ethernet ports 1 and 2 to receive 802.3x flow control pause frames:

```
Switch# configure terminal
Switch(config)# interface range fastethernet0/1 - 3 , gigabitethernet0/1 - 2
Switch(config-if-range)# flowcontrol receive on
```

If you enter multiple configuration commands while you are in interface range mode, each command is executed as it is entered. The commands are not batched together and executed after you exit interface range mode. If you exit interface range configuration mode while the commands are being executed, some commands might not be executed on all interfaces in the range. Wait until the command prompt reappears before exiting interface range configuration mode.

Configuring and Using Interface Range Macros

You can create an interface range macro to automatically select a range of interfaces for configuration. Before you can use the **macro** keyword in the **interface range macro** global configuration command string, you must use the **define interface-range** global configuration command to define the macro.

Beginning in privileged EXEC mode, follow these steps to define an interface range macro:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Define the interface-range macro, and save it in NVRAM. • The *macro_name* is a 32-character maximum character string. • A macro can contain up to five comma-separated interface ranges. • Each *interface-range* must consist of the same port type.	**define interface-range** *macro_name interface-range*
Step 3	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.	**no shutdown**

	Step	Command
Step 4	Select the interface range to be configured using the values saved in the interface-range macro called *macro_name.* You can now use the normal configuration commands to apply the configuration to all interfaces in the defined macro.	**interface range macro** *macro_name*
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Show the defined interface range macro configuration.	**show running-config | include define**
Step 7	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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

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

- Valid entries for *interface-range*:
  - **vlan** *vlan-ID - vlan-ID*, where the VLAN ID is 1 to 4094
  - **fastethernet** module/{first *port*} - {*last port*}, where the module is always 0
  - **gigabitethernet** module/{*first port*} - {*last port*}, where the module is always 0
  - **port-channel** *port-channel-number - port-channel-number*, where the *port-channel-number* is 1 to 48.

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

- You must add a space between the first interface number and the hyphen when entering an *interface-range*. For example, **gigabitethernet0/1 - 2** is a valid range; **gigabitethernet0/1-2** is not a valid range.
- The VLAN interfaces must have been configured with the **interface vlan** command. The **show running-config** privileged EXEC command displays the configured VLAN interfaces. VLAN interfaces not displayed by the **show running-config** command cannot be used as *interface-ranges*.
- All interfaces defined as in a range must be the same type (all Fast Ethernet ports, all Gigabit Ethernet ports, all EtherChannel ports, or all VLANs), but you can combine multiple interface types in a macro.

This example shows how to define an interface-range named *enet_list* to include ports 1 and 2 and to verify the macro configuration:

```
Switch# configure terminal
Switch(config)# define interface-range enet_list gigabitethernet0/1 - 2
Switch(config)# end
Switch# show running-config | include define
define interface-range enet_list GigabitEthernet0/1 - 2
```

This example shows how to create a multiple-interface macro named *macro1* and assign all of the interfaces in the range to a VLAN:

```
Switch# configure terminal
Switch# configure terminal
Switch(config)# define interface-range macro1 fastethernet0/1 - 2, gigabitethernet0/1 - 2
Switch(config)# interface range macro macro1
Switch(config-if-range)# switchport access vlan 20
Switch(config-if-range)# no shut
Switch(config-if-range)# end
```

This example shows how to enter interface range configuration mode for the interface-range macro *enet_list*:

```
Switch# configure terminal
Switch(config)# interface range macro enet_list
Switch(config-if-range)#
```

This example shows how to delete the interface-range macro *enet_list* and to verify that it was deleted

```
Switch# configure terminal
Switch(config)# no define interface-range enet_list
Switch(config)# end
Switch# show run | include define
Switch#
```

.Configuring Ethernet Interfaces

Default Ethernet Interface Configuration

Table 8-2 shows the Ethernet interface default configuration for NNIs, and Table 8-3 shows the Ethernet interface default configuration for UNIs and ENIs. For more details on the VLAN parameters listed in the table, see Chapter 11, "VLAN Configuration." For details on controlling traffic to the port, see Chapter 26, "Configuring Port-Based Traffic Control" in the *Cisco CGS 2520 Software Configuration Guide.*

Configuring Layer 2 Parameters

To configure Layer 2 parameters, if the interface is in Layer 3 mode, you must enter the **switchport** interface configuration command without any parameters to put the interface into Layer 2 mode. This shuts down the interface and then re-enables it, which might generate messages on the device to which

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

Table 8-2 shows the Ethernet interface default configuration for NNIs:

Table 8-2 Default Ethernet Configuration for NNIs

Feature	Default Setting
Operating mode	Layer 2 or switching mode (**switchport** command).
Allowed VLAN range	VLANs 1– 4094.
Default VLAN (for access ports)	VLAN 1 (Layer 2 interfaces only).
Native VLAN (for 802.1Q trunks)	VLAN 1 (Layer 2 interfaces only).
VLAN trunking	Switchport mode access (Layer 2 interfaces only).
Port enable state	Enabled.
Port description	None defined.
Speed	Autonegotiate.
Duplex mode	Autonegotiate.
802.3x flow control	Flow control is set to **receive**: **off**. It is always off for sent packets.
EtherChannel	Disabled on all Ethernet ports. See Chapter 15, "EtherChannel Configuration and Link State Tracking."
Port blocking (unknown multicast and unknown unicast traffic)	Disabled (not blocked) (only Layer 2 interfaces). See the Configuring Port Blocking" section in Chapter 26, "Configuring Port-Based Traffic Control" in the *Cisco CGS 2520 Software Configuration Guide*.
Broadcast, multicast, and unicast storm control	Disabled. See the "Default Storm Control Configuration" section in Chapter 26, "Configuring Port-Based Traffic Control" in the *Cisco CGS 2520 Software Configuration Guide*.
Port security	Disabled (only Layer 2 interfaces). See the "Default Port Security Configuration" section on page 26-10 in Chapter 26, "Configuring Port-Based Traffic Control" in the *Cisco CGS 2520 Software Configuration Guide*.
Port Fast	Disabled. See the "Default Optional Spanning-Tree Configuration" section on page 19-5 in Chapter 19, "Configuring Optional Spanning-Tree Features" in the *Cisco CGS 2520 Software Configuration Guide*.

Table 8-2 Default Ethernet Configuration for NNIs (continued)

Feature	Default Setting
Auto-MDIX	Enabled. **Note** The switch module might not support a pre-standard powered device—such as Cisco IP phones and access points that do not fully support 802.3af—if that powered device is connected to the switch module through a crossover cable. This is regardless of whether auto-MIDX is enabled on the switch port.
Power over Ethernet (PoE)	Enabled (auto).
Cisco Discovery Protocol (CDP)	Enabled.
VMPS	Not configured.

Table 8-3 Default Ethernet Configuration for UNIs and ENIs

Feature	Default Setting
Operating mode	Layer 2 or switching mode (**switchport** command).
Allowed VLAN range	VLANs 1– 4094.
Default VLAN (for access ports)	VLAN 1 (Layer 2 interfaces only).
Native VLAN (for 802.1Q trunks)	VLAN 1 (Layer 2 interfaces only).
VLAN trunking	Switchport mode access (Layer 2 interfaces only).
Dynamic VLAN	Enabled.
Port enable state	Disabled when no configuration file exists.
Port description	None defined.
Speed	Autonegotiate.
Duplex mode	Autonegotiate.
802.3x flow control	Flow control is set to **receive**: **off**. It is always off for sent packets.
EtherChannel	Disabled on all Ethernet ports. See Chapter 15, “EtherChannel Configuration and Link State Tracking.”
Port blocking (unknown multicast and unknown unicast traffic)	Disabled (not blocked) (only Layer 2 interfaces). See the See the XREF to “Configuring Port-Based Traffic Control” chapter, “Configuring Port Blocking” section.
Broadcast, multicast, and unicast storm control	Disabled. See the See the “Default Storm Control Configuration” section in Chapter 26, “Configuring Port-Based Traffic Control” in the *Cisco CGS 2520 Software Configuration Guide*.

Table 8-3 Default Ethernet Configuration for UNIs and ENIs (continued)

Feature	Default Setting
Port security	Disabled (only Layer 2 interfaces). See the Default Port Security Configuration" section in Chapter 26, "Configuring Port-Based Traffic Control" in the *Cisco CGS 2520 Software Configuration Guide*.
Auto-MDIX	Enabled.

Configuring the Port Type

By default, all the ports on the switch module are configured as NNIs.

You use the **port-type** interface configuration command to change the port types. You can change the ports on the switch module from NNIs to UNIs or ENIs. An ENI has the same characteristics as a UNI, but it can be configured to support CDP, STP, LLDP, and Etherchannel LACP.

When a port is changed from an NNI to a UNI or ENI, it inherits the configuration of the assigned VLAN, either in isolated or community mode. For more information about configuring UNI-ENI isolated and UNI-ENI community VLANs, see Chapter 11, "VLAN Configuration."

When you change a port from NNI to UNI or ENI or the reverse, any features exclusive to the port type revert to the default configuration. For Layer 2 protocols, such as STP, CDP, and LLDP, the default for UNIs and ENIs is disabled (although they can be enabled on ENIs) and the default for NNIs is enabled.

Note By default, the switch module sends keepalive messages on UNI s and ENIs and does not send keepalive messages on NNIs. Changing the port type from UNI or ENI to NNI or from NNI to UNI or ENI has no effect on the keepalive status. You can change the keepalive state from the default setting by entering the [**no**] **keepalive** interface configuration command. If you enter the **keepalive** command with no arguments, keepalive packets are sent with the default time interval (10 seconds) and number of retries (5). Entering the **no keepalive** command disables keepalive packets on the interface.

Beginning in privileged EXEC mode, follow these steps to configure the port type on an interface:

	Step	Command
Step 1	Enter global configuration mode	**configure terminal**
Step 2	Specify the interface to configure, and enter interface configuration mode.	**interface** *interface-id*
Step 3	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.	**no shutdown**
Step 4	Change a port to an ENI, NNI, or UNI.	**port-type** {**eni** | **nni** | **uni**}
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify the interface 802.3x flow control settings.	**show interfaces** *interface-id*
Step 7	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

Entering the **no port-type** or **default port-type** interface configuration command returns the port to the default state: UNI for Fast Ethernet ports and NNI for Gigabit Ethernet ports.

This example shows how to change a port from a UNI to an NNI and save it to the running configuration:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet0/1
Switch(config-if)# port-type nni
Switch(config-if)# no shutdown
5d20h: %SYS-5-CONFIG_I: Configured from console by console
Switch(config-if)# end
Switch# copy running-config startup-config
```

Configuring Interface Speed and Duplex Mode

Ethernet interfaces on the switch module operate at 10, 100, or 1000 Mbps and in either full- or half-duplex mode. In full-duplex mode, two stations can send and receive traffic at the same time. Normally, 10-Mbps ports operate in half-duplex mode, which means that stations can either receive or send traffic.

Switch Module models include combinations of Fast Ethernet (10/100-Mbps) ports, Gigabit Ethernet (10/100/1000-Mbps) ports, and small form-factor pluggable (SFP) module slots supporting SFP modules.

These sections describe how to configure the interface speed and duplex mode:

- Speed and Duplex Configuration Guidelines, page 8-22
- Setting the Interface Speed and Duplex Parameters, page 8-23

Speed and Duplex Configuration Guidelines

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

- You can configure interface speed on Fast Ethernet (10/100-Mbps) and Gigabit Ethernet (10/100/1000-Mbps) ports. You can configure Fast Ethernet ports to full-duplex, half-duplex, or to autonegotiate mode. You can configure Gigabit Ethernet ports to full-duplex mode or to autonegotiate. You also can configure Gigabit Ethernet ports to half-duplex mode if the speed is 10 or 100 Mbps. Half-duplex mode is not supported on Gigabit Ethernet ports operating at 1000 Mbps.
- With the exception of when 1000BASE-T SFP modules are installed in the SFP module slots, you cannot configure speed on SFP module ports, but you can configure speed to not negotiate (**nonegotiate**) if connected to a device that does not support autonegotiation.

  However, when a 1000BASE-T SFP module is in the SFP module slot, you can configure speed as 10, 100, or 1000 Mbps, or auto, but not as **nonegotiate**.

  On a 100BASE-FX SFP module, you cannot configure the speed as **nonegotiate**.
- You cannot configure duplex mode on SFP module ports; they operate in full-duplex mode except in these situations:
  - When a Cisco1000BASE-T SFP module is in the SFP module slot, you can configure duplex mode to **auto** or **full**. Half-duplex mode is supported with the **auto** setting.

  - When a Cisco100BASE-FX SFP module is in the SFP module slot, you can configure duplex mode to **half** or **full**. Although the **auto** keyword is available, it puts the interface in half-duplex mode (the default for this SFP module) because the 100BASE-FX SFP module does not support autonegotiation.

- If both ends of the line support autonegotiation, we highly recommend the default setting of **auto** negotiation.
- If one interface supports autonegotiation and the other end does not, configure duplex and speed on both interfaces; do not use the **auto** setting on the supported side.
- When STP is enabled and a port is reconfigured, the switch module can take up to 30 seconds to check for loops. The port LED is amber while STP reconfigures. On the CGR 2010 ESM, STP is supported on NNIs by default and can be enabled on ENIs. UNIs do not support STP.

Caution Changing the interface speed and duplex mode configuration might shut down and re-enable the interface during the reconfiguration.

Setting the Interface Speed and Duplex Parameters

Beginning in privileged EXEC mode, follow these steps to set the speed and duplex mode for a physical interface.

Note On dual-purpose ports, changing the interface type by entering the **media-type** interface configuration command removes the speed and duplex configurations. See the "Configuring a Dual-Purpose Port" section on page 8-29 for information about speed and duplex setting on these ports.

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

	Step	Command
Step 4	Enter the appropriate speed parameter for the interface: • Enter **100** or **1000** to set a specific speed for the interface. The **1000** keyword is available only for 10/100/1000 Mbps ports or SFP module ports with a 1000BASE-T SFP module. • Enter **auto** to enable the interface to autonegotiate speed with the connected device. If you use the **100** or the **1000** keywords with the **auto** keyword, the port autonegotiates only at the specified speeds. • The **nonegotiate** keyword is available only for SFP module ports. SFP module ports operate only at 1000 Mbps but can be configured to not negotiate if connected to a device that does not support autonegotiation. **Note** When a Cisco1000BASE-T SFP module is in the SFP module slot, the speed can be configured to **100**, **1000**, or to **auto**, but not to **nonegotiate**.	**speed** {**100** | **1000** | **auto** [**100** | **1000**] | **nonegotiate**}
Step 5	Enter the duplex parameter for the interface. Enable half-duplex mode (for interfaces operating only at 10 or 100 Mbps). You cannot configure half-duplex mode for interfaces operating at 1000 Mbps. You can configure the duplex setting when the speed is set to **auto**. This command is not available on SFP module ports with these exceptions: • If a Cisco 1000BASE-T SFP module is inserted, you can configure duplex to **auto** or to **full**. • If a Cisco 100BASE-FX SFP module is inserted, you can configure duplex to **full** or to **half**. Although the **auto** keyword is available, it puts the interface in half-duplex mode (the default).	**duplex** {**auto** | **full** | **half**}
Step 6	Return to privileged EXEC mode.	**end**
Step 7	Display the interface speed and duplex mode configuration.	**show interfaces** *interface-id*
Step 8	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

Use the **no speed** and **no duplex** interface configuration commands to return the interface to the default speed and duplex settings (autonegotiate). To return all interface settings to the defaults, use the **default interface** *interface-id* interface configuration command.

This example shows how to set the interface speed to 10 Mbps and the duplex mode to half on a 10/100 Mbps port:

```
Switch# configure terminal
Switch(config)# interface fasttethernet0/1/0
Switch(config-if)# no shutdown
Switch(config-if)# speed 10
Switch(config-if)# duplex half
```

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

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/2/0
Switch(config-if)# speed 100
```

Configuring a Power Management Mode on a PoE-Enabled Port

For most situations, the default configuration (auto mode) works well, providing plug-and-play operation. No further configuration is required. However, use the following procedure to give a Power over Ethernet-enabled port higher priority, to make it data only, or to specify a maximum wattage to disallow high-power powered devices on a port.

Note When you make PoE configuration changes, the port being configured drops power. Depending on the new configuration, the state of the other PoE ports, and the state of the power budget, the port might not be powered up again.

For example, assume that port 1 is in the auto and on state, and you configure it for static mode. The switch module removes power from port 1, detects the powered device, and repowers the port. If port 1 is in the auto and on state and you configure it with a maximum wattage of 10 W, the switch module removes power from the port and then redetects the powered device. The switch module repowers the port only if the powered device is a Class 1, Class 2, or a Cisco-only powered device.

Note Cisco IOS Release 12.2(53)EX and later supports enhanced PoE. You can use the power inline port maximum interface configuration command to support a device with the maximum power level of 20 watts.

Beginning in privileged EXEC mode, follow these steps to configure a power management mode on a PoE-capable port:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the physical port to be configured, and enter interface configuration mode.	**interface** *interface-id*

	Step	Command
Step 3	Configure the PoE mode on the port. The keywords have these meanings: • **auto**—Enable powered-device detection. If enough power is available, automatically allocate power to the PoE port after device detection. This is the default setting. (Optional) **max** *max-wattage*—Limits the power allowed on the port. The range is 4000 to 15400 mW. The default is 15400 mW. • **never**—Disable device detection, and disable power to the port. **Note** If a port has a Cisco powered device connected to it, do not use the **power inline never** command to configure the port. A false link-up can occur, placing the port into an error-disabled state. • **static**—Enable powered-device detection. Pre-allocate (reserve) power for a port before the switch module discovers the powered device. The switch module reserves power for this port even when no device is connected and guarantees that power will be provided on device detection. The switch module allocates power to a port configured in static mode before it allocates power to a port configured in auto mode.	**power inline** {**auto** [**max** *max-wattage*] | **never** | **static** [**max** *max-wattage*]}
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Display PoE status for the switch module or for the specified interface.	**show power inline** [*interface-id*]
Step 6	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

For information about the output of the show power inline user EXEC command, see the *Cisco IOS Interface Command Reference, Release 12.2*. For more information about PoE-related commands, see "Troubleshooting Power over Ethernet Switch Module Ports" section on page 18-3.

Budgeting Power for Devices Connected to a PoE Port

The PoE power budget for the CGR 2010 ESM is shared among the modules installed in the Cisco CGR 2010 router chassis. The maximum PoE power for the whole router chassis is 61.6W. If there are two switch modules inserted into the router chassis, the total maximum power availability for both modules would be 61.6W, and one of the modules may get only a portion of that power budget.

Caution You should carefully plan your switch module power budget and make certain not to oversubscribe the power supply.

Note When you manually configure the power budget, you must also consider the power loss over the cable between the switch module and the powered device.

The switch module supports four PoE ports in the Copper FastEthernet SKU. These four ports are always the first four ports (FE0/1 to FE0/4) among the total eight FastEthernet ports.

When Cisco powered devices are connected to PoE ports, the switch module uses Cisco Discovery Protocol (CDP) to determine the actual power consumption of the devices, and the switch module adjusts the power budget accordingly. The CDP protocol works with Cisco powered devices and does not apply to IEEE third-party powered devices. For these devices, when the switch module grants a power request, the switch module adjusts the power budget according to the powered-device IEEE classification.

If the powered device is a Class 0 (class status unknown) or a Class 3, the switch module budgets 15,400 milliwatts for the device, regardless of the actual amount of power needed. If the powered device reports a higher class than its actual consumption or does not support power classification (defaults to Class 0), the switch module can power fewer devices because it uses the IEEE class information to track the global power budget.

By using the **power inline consumption** *wattage* configuration command, you can override the default power requirement specified by the IEEE classification. The difference between what is mandated by the IEEE classification and what is actually needed by the device is reclaimed into the global power budget for use by additional devices. You can then extend the switch module power budget and use it more effectively.

For example, if the switch module budgets 15,400 milliwatts on each PoE port, you can connect only four Class 0 powered devices. If the device is actually using 5,000 milliwatts, you can connect up to 12 devices.

When you enter the **power inline consumption default** *wattage* command or the **no power inline consumption default** global configuration command, or the **power inline consumption** *wattage* command or the **no power inline consumption** interface configuration command this caution message appears:

Caution Interface: Misconfiguring the ‘power inline consumption/allocation’ command may cause damage to the switch module and void your warranty. Take precaution not to oversubscribe the power supply.

We recommend you enable power policing.

If the power supply is over-subscribed to by up to 20 percent, the switch module continues to operate but its reliability is reduced. If the power supply is subscribed to by more than 20 percent, the short-circuit protection circuitry triggers and shuts the switch module down.

For more information about the IEEE power classifications, see the “Power Over Ethernet Ports” section on page 8-7.

Beginning in privileged EXEC mode, follow these steps to configure the amount of power budgeted to a powered device connected to each PoE port on a switch module:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	(Optional) Disable CDP.	**no cdp run**
Step 3	Configure the power consumption of powered devices connected to each the PoE port on the switch module. The range for each device is 4000 to 15400 mW. The default is 15400 mW.	**power inline consumption default** *wattage*
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Display the power consumption status.	**show power inline consumption**
Step 6	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To return to the default setting, use the **no power inline consumption** default global configuration command.

Note The CGR 2010 ESM does not support the **power inline port priority** command.

Beginning in privileged EXEC mode, follow these steps to configure amount of power budgeted to a powered device connected to a specific PoE port:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	(Optional) Disable CDP.	**no cdp run**
Step 3	Specify the physical port to be configured, and enter interface configuration mode.	**interface** *interface-id*
Step 4	Configure the power consumption of a powered device connected to a PoE port on the switch module. The range for each device is 4000 to 15400 mW. The default is 15400 mW. **Note** When you use this command, we recommend you also enable power policing.	**power inline consumption** *wattage*
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Display the power consumption status.	**show power inline consumption**
Step 7	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To return to the default setting, use the **no power inline consumption** interface configuration command.

Beginning in privileged EXEC mode, follow these steps to configure amount of power budgeted to a powered device connected to a specific PoE port:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	(Optional) Disable CDP.	**no cdp run**
Step 3	Specify the physical port to be configured, and enter interface configuration mode.	**interface** *interface-id*
Step 4	Configure the power consumption of a powered device connected to a PoE port on the switch module. The range for each device is 4000 to 15400 mW. The default is 15400 mW.	**power inline consumption** *wattage*
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Display the power consumption status.	**show power inline consumption**
Step 7	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To return to the default setting, use the **no power inline consumption** interface configuration command.

For information about the output of the **show power inline consumption** privileged EXEC command, see the *Cisco IOS Interface Command Reference, Release 12.2*.

Configuring a Dual-Purpose Port

The switch module provides dual-purpose ports that can be configured as 10/100/100 ports or as small form-factor pluggable (SFP) module ports. Each dual-purpose port is considered as a single interface with dual front ends (an RJ-45 connector and an SFP module connector).

Note Even when operating at 10 or 100 Mbps, the dual-purpose ports (and the SFP-only module ports) use the frame size that is set with the **system mtu jumbo** global configuration command.

Each dual-purpose port is considered as a single interface with dual front ends (an RJ-45 connector and an SFP module connector). The dual front ends are not redundant interfaces; the switch module activates only one connector of the pair.

By default, the dual-purpose ports are user-network interfaces (UNIs) and the SFP-only module ports are network node interfaces (NNIs).

By default, the switch module dynamically selects the dual-purpose port media type that first links up. However, you can use the **media-type** interface configuration command to manually select the RJ-45 connector or the SFP-module connector. In **auto-select** mode, the switch module gives preference to SFP mode if both copper and fiber-optic signals are simultaneously detected.

Beginning in privileged EXEC mode, follow these steps to select which dual-purpose media type to activate. This procedure is optional.

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the dual-purpose port to be configured, and enter interface configuration mode.	**interface** *interface-id*
Step 3	Select the active interface and media type of a dual-purpose port. The keywords have these meanings: • **auto-select**—The switch module dynamically selects the media type. This is the default. When a linkup is achieved, the switch module disables the other type until the active link goes down. When the active link goes down, the switch module enables both types until one of them links up. In auto-select mode, the switch module configures both types with autonegotiation of speed and duplex (the default). • **rj45**—The switch module disables the SFP module interface. If you connect a cable to the SFP port, it cannot attain a link even if the RJ-45 side is down or is not connected. In this mode, the dual-purpose port behaves like a 10/100/1000BASE-TX interface. You can configure the speed and duplex settings consistent with this interface type. • **sfp**—The switch module disables the RJ-45 interface. If you connect a cable to the RJ-45 port, it cannot attain a link even if the SFP side is down or if the SFP module is not present. Based on the type of installed SFP module, you can configure the speed and duplex settings consistent with this interface type.	**media-type** {**auto-select** | **rj45** | **sfp**}
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your setting.	**show interfaces** *interface-id* **transceiver properties**
Step 6	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To return to the default setting, use the **no media-type** interface configuration command.

Changing the interface type removes the speed and duplex configurations. The switch module configures both media types to autonegotiate speed and duplex (the default). If you configure **auto-select**, you cannot configure the **speed** and **duplex** interface configuration commands.

When you configure **sfp** or **rj45** media type, the non-configured type is disabled, even if there is a connector installed in that interface and no connector in the configured one.

When the media type is **auto-select**, the switch module uses these criteria to select the type:

Note An SFP is not *installed* until it has a fiber-optic or copper cable plugged in.

- If only one connector is installed, that interface is active and remains active until the media is removed or the switch module is reloaded.
- If you install both types of media in an enabled dual-purpose port, the switch module selects the active link based on which type is installed first.
- If both media are installed in the dual-purpose port, and the switch module is reloaded or the port is disabled and then reenabled through the **shutdown** and the **no shutdown** interface configuration commands, the switch module gives preference to the SFP module interface.

See the **media-type** interface configuration command in the *Cisco IOS Interface Command Reference, Release 12.2* for more information.

Configuring IEEE 802.3x Flow Control

802.3x flow control enables connected Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If one port experiences congestion and cannot receive any more traffic, it notifies the other port by sending a pause frame to stop sending until the condition clears. Upon receipt of a pause frame, the sending device stops sending any data packets, which prevents any loss of data packets during the congestion period.

Note Ports can receive, but not send, pause frames.

You use the **flowcontrol** interface configuration command to set the interface's ability to **receive** pause frames to **on**, **off**, or **desired**. The default state is **off**.

When set to **desired**, an interface can operate with an attached device that is required to send flow-control packets or with an attached device that is not required to but can send flow-control packets.

These rules apply to 802.3x flow control settings on the device:

- **receive on** (or **desired**): The port cannot send pause frames but can operate with an attached device that is required to or can send pause frames; the port can receive pause frames.
- **receive off**: 802.3x flow control does not operate in either direction. In case of congestion, no indication is given to the link partner, and no pause frames are sent or received by either device.

Note For details on the command settings and the resulting 802.3x flow control resolution on local and remote ports, see the **flowcontrol** interface configuration command in the *Cisco IOS Interface Command Reference, Release 12.2*.

Beginning in privileged EXEC mode, follow these steps to configure 802.3x flow control on an interface:

	Step	Command
Step 1	Enter global configuration mode	**configure terminal**
Step 2	Specify the physical interface to be configured, and enter interface configuration mode.	**interface** *interface-id*
Step 3	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.	**no shutdown**
Step 4	Configure the 802.3x flow control mode for the port.	**flowcontrol** {**receive**} {**on** | **off** | **desired**}
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify the interface 802.3x flow control settings.	**show interfaces** *interface-id*
Step 7	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To disable 802.3x flow control, use the **flowcontrol receive off** interface configuration command.

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

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

Configuring Auto-MDIX on an Interface

When automatic medium-dependent interface crossover (auto-MDIX) is enabled on an interface, the interface automatically detects the required cable connection type (straight through or crossover) and configures the connection appropriately. When connecting switches without the auto-MDIX feature, you must use straight-through cables to connect to devices such as servers, workstations, or routers and crossover cables to connect to other switches or repeaters. With auto-MDIX enabled, you can use either type of cable to connect to other devices, and the interface automatically corrects for any incorrect cabling. For more information about cabling requirements, see the hardware installation guide.

Auto-MDIX is enabled by default. When you enable auto-MDIX, you must also set the speed and duplex on the interface to **auto** so that the feature operates correctly. Auto-MDIX is supported on all 10/100 and 10/100/1000 Mbps interfaces and on Cisco 10/100/1000 BASE-T/TX SFP module interfaces. It is not supported on 1000 BASE-SX or -LX SFP module interfaces.

Table 8-4 shows the link states that result from auto-MDIX settings and correct and incorrect cabling.

Table 8-4 Link Conditions and Auto-MDIX Settings

Local Side Auto-MDIX	Remote Side Auto-MDIX	With Correct Cabling	With Incorrect Cabling
On	On	Link up	Link up
On	Off	Link up	Link up
Off	On	Link up	Link up
Off	Off	Link up	Link down

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

	Step	Command
Step 1	Enter global configuration mode	**configure terminal**
Step 2	Specify the physical interface to be configured, and enter interface configuration mode.	**interface** *interface-id*
Step 3	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.	**no shutdown**
Step 4	Configure the interface to autonegotiate speed with the connected device.	**speed auto**
Step 5	Configure the interface to autonegotiate duplex mode with the connected device.	**duplex auto**
Step 6	Enable auto-MDIX on the interface.	**mdix auto**
Step 7	Return to privileged EXEC mode.	**end**
Step 8	Verify the operational state of the auto-MDIX feature on the interface.	**show controllers ethernet-controller** *interface-id* **phy**
Step 9	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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

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

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no shutdown
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

Adding a Description for an Interface

You can add a description about an interface to help you remember its function. The description appears in the output of these privileged EXEC commands: **show configuration**, **show running-config**, and **show interfaces**.

Beginning in privileged EXEC mode, follow these steps to add a description for an interface:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the interface for which you are adding a description, and enter interface configuration mode.	**interface** *interface-id*
Step 3	Add a description (up to 240 characters) for an interface.	**description** *string*

	Step	Command
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entry.	**show interfaces** *interface-id* **description** or **show running-config**
Step 6	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

Use the **no description** interface configuration command to delete the description.

This example shows how to add a description on a port and how to verify the description:

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# description Connects to Marketing
Switch(config-if)# end
Switch# show interfaces gigabitethernet0/2 description
Interface Status         Protocol Description
Gi 0/2   admin down     down     Connects to Marketing
```

Configuring Layer 3 Interfaces

The switch module must be running the IP services image to support Layer 3 interfaces. The CGR 2010 ESM supports these types of Layer 3 interfaces:

- SVIs: You should configure SVIs for any VLANs for which you want to route traffic. SVIs are created when you enter a VLAN ID following the **interface vlan** global configuration command. To delete an SVI, use the **no interface vlan** global configuration command. You cannot delete interface VLAN 1.

  Note When you create an SVI, it does not become active until it is associated with a physical port. For information about assigning Layer 2 ports to VLANs, see Chapter 11, "VLAN Configuration."

- Routed ports: Routed ports are physical ports configured to be in Layer 3 mode by using the **no switchport** interface configuration command.
- Layer 3 EtherChannel ports: EtherChannel interfaces made up of routed ports.

  EtherChannel port interfaces are described in Chapter 15, "EtherChannel Configuration and Link State Tracking."

A Layer 3 switch can have an IP address assigned to each routed port and SVI.

There is no defined limit to the number of SVIs and routed ports that can be configured in a switch module. However, the interrelationship between the number of SVIs and routed ports and the number of other features being configured might have an impact on CPU usage because of hardware limitations. If the switch module is using maximum hardware resources, attempts to create a routed port or SVI have these results:

- If you try to create a new routed port, the switch module generates a message that there are not enough resources to convert the interface to a routed port, and the interface remains as a switch port.
- If you try to create an extended-range VLAN, an error message is generated, and the extended-range VLAN is rejected.
- If the switch module attempts to boot up with a configuration that has more VLANs and routed ports than hardware can support, the VLANs are created, but the routed ports are shut down, and the switch module sends a message that this was due to insufficient hardware resources.

All Layer 3 interfaces require an IP address to route traffic. This procedure shows how to configure an interface as a Layer 3 interface and how to assign an IP address to an interface.

Note If the physical port is in Layer 2 mode (the default), you must enter the **no switchport** interface configuration command to put the interface into Layer 3 mode. Entering a **no switchport** command disables and then re-enables the interface, which might generate messages on the device to which the interface is connected. Furthermore, when you put an interface that is in Layer 2 mode into Layer 3 mode, the previous configuration information related to the affected interface might be lost, and the interface is returned to its default configuration

Beginning in privileged EXEC mode, follow these steps to configure a Layer 3 interface:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the interface to be configured as a Layer 3 interface, and enter interface configuration mode.	**interface** {{**fastethernet** | **gigabitethernet**} *interface-id*} | {**vlan** *vlan-id*} | {**port-channel** *port-channel-number*}
Step 3	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.	**no shutdown**
Step 4	For physical ports only, enter Layer 3 mode.	**no switchport**
Step 5	Configure the IP address and IP subnet.	**ip address** *ip_address subnet_mask*
Step 6	Enable the interface.	**no shutdown**
Step 7	Return to privileged EXEC mode.	**end**
Step 8	Verify the configuration.	**show interfaces** [*interface-id*] **show ip interface** [*interface-id*] **show running-config interface** [*interface-id*]
Step 9	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To remove an IP address from an interface, use the **no ip address** interface configuration command.

This example shows how to configure a port as a routed port and to assign it an IP address:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.20.135.21 255.255.255.0
```

Configuring the System MTU

The default maximum transmission unit (MTU) size for frames received and sent on all interfaces on the switch is 1500 bytes. You can increase the MTU size for all interfaces operating at 10 or 100 Mbps by using the **system mtu** global configuration command. You can increase the MTU size to support jumbo frames on all Gigabit Ethernet interfaces by using the **system mtu jumbo** global configuration command. You can change the MTU size for routed ports by using the **system mtu routing** global configuration command.

Note You cannot configure a routing MTU size that exceeds the system MTU size. If you change the system MTU size to a value smaller than the currently configured routing MTU size, the configuration change is accepted, but not applied until the next switch module reset. When the configuration change takes effect, the routing MTU size automatically defaults to the new system MTU size.

Gigabit Ethernet ports are not affected by the **system mtu** command. Fast Ethernet ports are not affected by the **system mtu jumbo** command because jumbo frames are not supported on 10/100 interfaces, including 100BASE-FX and 100BASE-BX SFP modules. If you do not configure the **system mtu jumbo** command, the setting of the **system mtu** command applies to all Gigabit Ethernet interfaces.

You cannot set the MTU size for an individual interface; you set it for all 10/100 or all Gigabit Ethernet interfaces on the switch module. When you change the system MTU size, you must reset the switch module before the new configuration takes effect. The **system mtu routing** command does not require a switch module reset to take effect.

Note The system MTU setting is saved in the switch module environmental variable in NVRAM and becomes effective when the switch module reloads. The MTU settings you enter with the **system mtu** and **system mtu jumbo** commands are not saved in the switch module IOS configuration file, even if you enter the **copy running-config startup-config** privileged EXEC command. If you use TFTP to configure a new switch module by using a backup configuration file and want the system MTU to be other than the default, you must explicitly configure the **system mtu** and **system mtu jumbo** settings on the new switch module and then reload the switch module.

Frames sizes that can be received by the switch module CPU are limited to 1998 bytes, no matter what value was entered with the **system mtu** or **system mtu jumbo** commands. Although frames that are forwarded are typically not received by the CPU, in some cases packets are sent to the CPU, such as traffic sent to control traffic, SNMP, Telnet, or routing protocols.

Because the switch module does not fragment packets, it drops:

- Switched packets larger than the packet size supported on the *egress* interface.
- Routed packets larger than the routing MTU value.

For example, if the **system mtu** value is 1998 bytes and the **system mtu jumbo** value is 5000 bytes, packets up to 5000 bytes can be received on interfaces operating at 1000 Mbps. However, although a packet larger than 1998 bytes can be received on an interface operating at 1000 Mbps, if its destination interface is operating at 10 or 100 Mbps, the packet is dropped.

Routed packets are subjected to MTU checks on the sending ports. The MTU value used for routed ports is derived from the configured **system mtu** value (not the **system mtu jumbo** value). That is, the routed MTU is never greater than the system MTU for any VLAN. The routing protocols use the system MTU value when negotiating adjacencies and the MTU of the link. For example, the Open Shortest Path First

(OSPF) protocol uses this MTU value before setting up an adjacency with a peer router. To view the MTU value for routed packets for a specific VLAN, use the **show platform port-asic mvid** privileged EXEC command.

Note If Layer 2 Gigabit Ethernet interfaces are configured to accept frames greater than the 10/100 interfaces, jumbo frames received on a Layer 2 Gigabit Ethernet interface and sent on a Layer 2 10/100 interface are dropped.

Beginning in privileged EXEC mode, follow these steps to change the MTU size for all 10/100 or Gigabit Ethernet interfaces:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	(Optional) Change the MTU size for all interfaces on the switch module that are operating at 10 or 100 Mbps. The range is 1500 to 1998 bytes; the default is 1500 bytes.	**system mtu** *bytes*
Step 3	(Optional) Change the MTU size for all Gigabit Ethernet interfaces on the switch module. The range is 1500 to 9000 bytes; the default is 1500 bytes.	**system mtu jumbo** *bytes*
Step 4	(Optional) Change the system MTU for routed ports. The range is 1500 to the system MTU value, the maximum MTU that can be routed for all ports. Although larger packets can be accepted, they cannot be routed.	**system mtu routing** *bytes*
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Save your entries in the configuration file.	**copy running-config startup-config**
Step 7	Reload the operating system.	**reload**

If you enter a value that is outside the allowed range for the specific type of interface, the value is not accepted.

Once the switch module reloads, you can verify your settings by entering the **show system mtu** privileged EXEC command.

This example shows how to set the maximum packet size for a Gigabit Ethernet port to 1800 bytes:

```
Switch(config)# system mtu jumbo 1800
Switch(config)# exit
Switch# reload
```

This example shows the response when you try to set Gigabit Ethernet interfaces to an out-of-range number:

```
Switch(config)# system mtu jumbo 25000

% Invalid input detected at '^' marker.
```

Monitoring and Maintaining the Interfaces

These sections contain interface monitoring and maintenance information:

Monitoring Interface Status

Commands entered at the privileged EXEC prompt display information about the interface, including the versions of the software and the hardware, the configuration, and statistics about the interfaces. Table 8-5 lists some of these interface monitoring commands. (You can display the full list of **show** commands by using the **show ?** command at the privileged EXEC prompt.) These commands are fully described in the *Cisco IOS Interface Command Reference, Release 12.2*.

Table 8-5 Show Commands for Interfaces

Command	Description
show interfaces [*interface-id*]	Display the status and configuration of all interfaces or a specific interface.
show interfaces *interface-id* **status** [**err-disabled**]	Display interface status or a list of interfaces in an error-disabled state.
show interfaces [*interface-id*] **switchport**	Display administrative and operational status of switching mode. You can use this command to find out if a port is in routing or in switching mode.
show interfaces [*interface-id*] **description**	Display the description configured on an interface or all interfaces and the interface status.
show ip interface [*interface-id*]	Display the usability status of all interfaces configured for IP routing or the specified interface.
show interface [*interface-id*] **stats**	Display the input and output packets by the switching path for the interface.

Table 8-5 Show Commands for Interfaces (continued)

Command	Description
show interfaces [*interface-id]* **transceiver** [**detail** | **dom-supported-list** | **module** *number* | **properties** | **threshold-table**]	Display these physical and operational status about an SFP module: • *interface-id*–(Optional) Display configuration and status for a specified physical interface. • **detail–**(Optional) Display calibration properties, including high and low numbers and any alarm information for any Digital Optical Monitoring (DoM)-capable transceiver if one is installed in the switch module. • **dom-supported-list–**(Optional) List all supported DoM transceivers. • **module** *number***–**(Optional) Limit display to interfaces on module on the switch module. The range is 1 to 9. This option is not available if you entered a specific interface ID. • **properties–**(Optional) Display speed, duplex, and inline power settings on an interface • **threshold-table–**(Optional) Display alarm and warning threshold table
show interfaces [*interface-id*] [{**transceiver properties** | **detail**}] *module number*]	Display physical and operational status about an SFP module.
show port-type [**eni** | **nni** | **uni**]	Display interface type information for the Cisco ME switch.
show running-config interface [*interface-id*]	Display the running configuration in RAM for the interface.
show version	Display the hardware configuration, software version, the names and sources of configuration files, and the boot images.
show controllers ethernet-controller *interface-id* **phy**	Display the operational state of the auto-MDIX feature on the interface.

Clearing and Resetting Interfaces and Counters

Table 8-6 lists the privileged EXEC mode **clear** commands that you can use to clear counters and reset interfaces.

Table 8-6 Clear Commands for Interfaces

Command	Description
clear counters [*interface-id*]	Clear interface counters.
clear interface *interface-id*	Reset the hardware logic on an interface.
clear line [*number* | **console 0** | **vty** *number*]	Reset the hardware logic on an asynchronous serial line.

To clear the interface counters shown by the **show interfaces** privileged EXEC command, use the **clear counters** privileged EXEC command. The **clear counters** command clears all current interface counters from the interface unless you specify optional arguments that clear only a specific interface type from a specific interface number.

Note The **clear counters** privileged EXEC command does not clear counters retrieved by using Simple Network Management Protocol (SNMP), but only those seen with the **show interface** privileged EXEC command.

Shutting Down and Restarting the Interface

Shutting down an interface disables all functions on the specified interface and marks the interface as unavailable on all monitoring command displays. This information is communicated to other network servers through all dynamic routing protocols. The interface is not mentioned in any routing updates.

Beginning in privileged EXEC mode, follow these steps to shut down an interface:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Select the interface to be configured.	**interface** {**vlan** *vlan-id*} | {{**fastethernet** | **gigabitethernet**} *interface-id*} | {**port-channel** *port-channel-number*}
Step 3	Shut down an interface.	**shutdown**
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entry.	**show running-config**

Use the **no shutdown** interface configuration command to enable an interface.

To verify that an interface is disabled, enter the **show interfaces** privileged EXEC command. A disabled interface is shown as *administratively down* in the display.

EtherChannel Configuration Between the Switch Module and the Host Router

This chapter describes how to configure the backplane interface PortChannel48, which provides communication between the host router and the switch module. It contains the following topics:

About the Backplane PortChannel48 Interface

The CGR 2010 ESM is inserted into the Cisco CGR 2010 Router. The switch module's backplane interface is called *PortChannel48*. PortChannel48 is the backplane interface connected to the CGR 2010 Router and provides communication between the host router and the switch module.

The PortChannel48 interface consists of eight 10/100 Fast Ethernet physical links that are grouped together to create a FastEtherChannel. PortChannel48 is created automatically when the switch module boots up.

Note It is recommended that all eight interfaces should be EtherChannel members and users are discouraged from removing any of the eight interfaces from the EtherChannel.

You can configure these interfaces like any other interface with the important exception that you cannot delete the system-created PortChannel48 interface.

You can change the PortChannel48 interface configuration from trunk mode to access mode (that is, non-trunk mode), or configure the PortChannel48 interface as a Layer 3 interface by configuring an IP address on the interface. For details, see "Configuring the Backplane PortChannel48 Interface" section on page 9-2.

Once a port is designated as a trunk port, it will forward and receive tagged frames.Frames belonging to the native VLAN do *not* carry VLAN tags when sent over the trunk. Conversely, if an untagged frame is received on a trunk port, the frame is associated with the native VLAN for this port.

The backplane PortChannel48 interfaces to the CGR 2010 host router. The router does not recognize spanning tree BPDUs; the spanning Tree Protocol is disabled on the PortChannel48 interface.

PortChannel48 Defaults

By default, the PortChannel48 interface comes up in Layer 2 trunk mode, with 802.1Q trunk encapsulation. 802.1Q is the only encapsulation method supported on the switch module.

Here is how the typical PortChannel and individual physical configuration looks when the switch module comes up the first time:

```
!
interface Port-channel48
port-type nni
switchport mode trunk
!

interface FastEthernet0/5
port-type nni
switchport mode trunk
channel-group 48 mode on
```

By default, the PortChannel48 interface is created in Layer 2 trunk mode, which means that the switch module operates in Layer 2 trunk mode with 802.1Q encapsulation carrying VLAN1 by default. This PortChannel48 interface supports load-balancing across multiple physical links, in the same way as the regular user-configured EtherChannel does, using the following parameters:

- Destination IP address
- Destination MAC address
- Source IP address XOR with destination IP address
- Source MAC address XOR with destination MAC address
- Source IP address
- Source MAC address (default mode)

Configuring the Backplane PortChannel48 Interface

By default, the switch module comes up in Layer 2 trunk mode. This section describes how to configure the PortChannel48 interface for the switch module for each of the following modes:

- Layer 3 routing mode
- Layer 2 trunk mode
- Layer 2 access mode

Configuring the PortChannel48 Interface for Layer 3 Routing Mode

This section describes how to change from the default Layer 2 trunk mode to Layer 3 routing mode:

```
switch# show run interface f0/5
interface FastEthernet0/5
description: Member of internal backplane interface Port-channel48. Use caution while
changing the configuration.
port-type nni
switchport mode trunk
channel-group 48 mode on
end
```

```
switch# configure terminal
switch(config)# interface range f0/5-12
description: interfaces FE0/5 to FE0/12 apply to the Fiber model; interfaces FE0/9 to
FE0/16 apply to the Copper model
switch(config-if)# no channel-group 48 mode on
switch(config-if)# no switchport
switch(config-if)# end
switch(config)# interface port-channel 48
switch(config-if)# no switchport
switch(config-if)# ip address 209.165.200.225 255.0.0.0
switch(config-if)# ^Z
switch(config)# interface f0/5
switch(config-if)# channel-group 48 mode on
description: repeat for all 8 ports from 0/5 to 0/12
switch(config-if)# ^Z
switch#
switch# show interface port-channel 48
interface Port-channel48
description: "Internal backplane interface. Use caution while changing the
configuration"
port-type nni
no switchport
ip address 209.165.200.225 255.0.0.0
end
```

Configuring the PortChannel48 Interface for Layer 2 Trunk Mode

These commands configure the PortChannel in Layer 2 Trunk mode.

Method 1

This command configures both the PortChannel48 interface and its member ports in trunk mode.

```
configure terminal
default interface po48
```

Method 2

Note that every port from FE0/5 to FE0/12 (on the Fiber Model) and ports FE0/9 to FE0/16 (on the Copper Model) should be configured as shown here:

```
interface Port-channel48
port-type nni
switchport mode trunk
!
interface FastEthernet0/5
port-type nni
switchport mode trunk
channel-group 48 mode on
```

Configuring the PortChannel48 Interface for Layer 2 Access Mode

These commands configure the PortChannel in Layer 2 Access mode. Note that every port from FE0/5 to FE0/12 (on the Fiber Model) and ports FE0/9 to FE0/16 (on the Copper Model) should be configured as shown here:

```
interface InternalPort-channel48
switchport mode access
!
!#Incoming switch module interface connected
interface FastEthernet0/5
switchport mode access
channel-group 48 mode on
```

Sample Gigabit Ethernet Interface Configuration on the CGR 2010 Router

This section describes the Gigabit Ethernet configuration required on the host CGR 2010 router to implement the PortChannel48 interface on the router.

Interface **GigabitEthernet0/**<*slot 0 or 2*>**/0** is the backplane interface connected to the switch module. This interface can also have subinterfaces for each of the networks.

Interface to Receive Routed Traffic for Network 20.70.0.0

```
interface GigabitEthernet0/0/0
ip address 20.70.1.1 255.255.0.0
```

Interface to Receive Bridge Traffic on bridge-group 60

```
interface GigabitEthernet0/0/0
ip address 20.70.1.1 255.255.0.0
duplex auto
speed auto
media-type rj45
bridge-group 60
```

Backplane Subinterface to Receive Bridged Traffic on VLAN 60

```
interface GigabitEthernet0/0/0
ip address 20.70.1.1 255.255.0.0
!
interface GigabitEthernet0/0/0.60
encapsulation dot1Q 60
bridge-group 60
!
```

Backplane Subinterface to Receive Routed Traffic on VLAN 70

```
interface GigabitEthernet0/0/0.70
ip address 40.70.1.1 255.255.0.0
```

Specifying the Static Route for the Network

```
ip route 40.70.0.0 255.255.0.0 GigabitEthernet0/0/0
```

Smartports Macros Configuration

This chapter describes how to configure and display Smartports macros. It contains the following topics:

Understanding Smartports Macros

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

Each Smartports macro is a set of CLI commands. The switch module 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 a system default (which cannot be edited by the user).

Configuring Smartports Macros

Default Smartports Configuration

There are no Smartports macros enabled on the switch module.

Table 10-1 Default Smartports Macros

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

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

Smartports Configuration Guidelines

- You can apply a macro globally or to a specific switch module 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 module 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 module or interface, the macro name is automatically added to the switch module 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.

Applying Smartports Macros

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

	Step	Command
Step 1	Display the Cisco-default Smartports macros embedded in the switch module software.	**show parser macro**
Step 2	Display the specific macro that you want to apply.	**show parser macro name** *macro-name*
Step 3	Enter global configuration mode.	**configure terminal**

	Step	Command
Step 4	Apply each individual command defined in the macro to the switch module 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 **$** require a unique parameter value. You can use the **macro global apply** *macro-name* **?** command to display a list of any required values for the macro. If you apply a macro without entering the keyword values, the commands are invalid and are not applied. (Optional) Specify unique parameter values that are specific to the switch module. You can enter up to three keyword-value pairs. Parameter keyword matching is case sensitive. The corresponding value replaces all matching occurrences of the keyword.	**macro global** {**apply** | **trace**} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]
Step 5	(Optional) Enter interface configuration mode, and specify the interface on which to apply the macro.	**interface** *interface-id*
Step 6	(Optional) Clear all configuration from the specified interface.	**default interface** *interface-id*
Step 7	Apply each individual command defined in the macro to the port by entering **macro apply** *macro-name*. Specify **macro trace** *macro-name* to apply and to debug a macro to find any syntax or configuration errors. Append the macro with the required values by using the **parameter** *value* keywords. Keywords that begin with **$** 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 module. 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.	**macro** {**apply** | **trace**} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]
Step 8	Return to privileged EXEC mode.	**end**

	Step	Command
Step 9	Verify that the macro is applied to an interface.	**show running-config interface** *interface-id*
Step 10	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

You can delete the **cisco-cg-password** and **cisco-sniffer** global macros on a switch module 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.

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'
```

Displaying Smartports Macros

To display the Smartports macros, use one or more of the privileged EXEC commands in Table 10-2.

Table 10-2 Commands for Displaying Smartports Macros

Command	Description
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.

VLAN Configuration

This chapter describes how to configure normal-range VLANs (VLAN IDs 1 to 1005) and extended-range VLANs (VLAN IDs 1006 to 4094) on the CGR 2010 ESM. It includes information about VLAN membership modes, VLAN configuration modes, VLAN trunks, and dynamic VLAN assignment from a VLAN Membership Policy Server (VMPS).

Note For complete syntax and usage information for the commands used in this chapter, see the online *Cisco IOS Interface Command Reference, Release 12.2*.

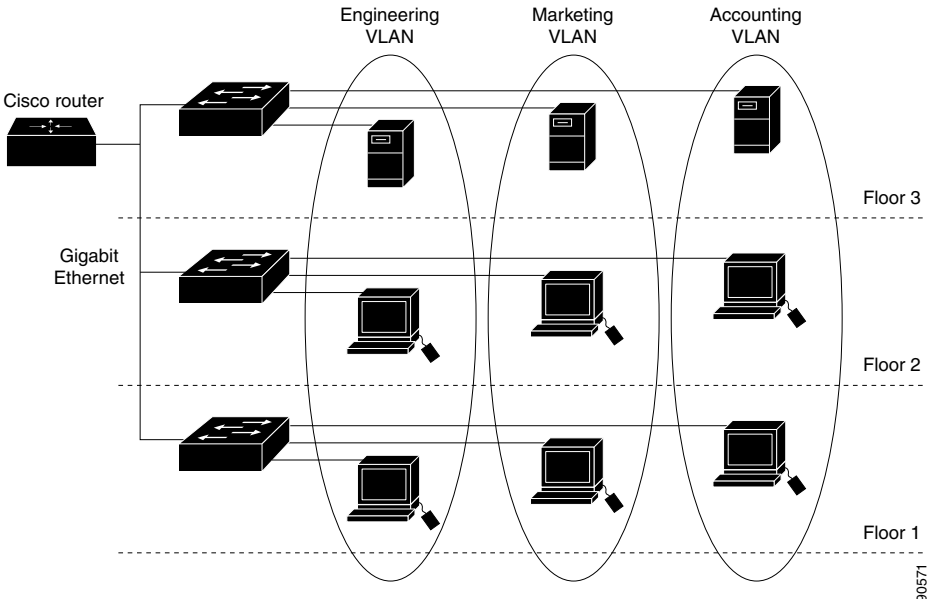
Understanding VLANs

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch module port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN.

Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router, as shown in Figure 11-1. Because a VLAN is considered a separate logical network, it contains its own bridge MIB information and can support its own implementation of spanning tree. See Chapter 17, “Configuring STP” in the *Cisco CGS 2520 Software Configuration Guide*.

Figure 11-1 shows an example of VLANs segmented into logically defined networks.

Figure 11-1 VLANs as Logically Defined Networks



VLANs are often associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Interface VLAN membership on the switch module is assigned manually on an interface-by-interface basis. When you assign switch module interfaces to VLANs by using this method, it is known as interface-based, or static, VLAN membership.

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

Traffic between VLANs must be routed. Switch modules that are running the IP services image can route traffic between VLANs by using Switch Virtual Interfaces (SVIs). To route traffic between VLANs, an SVI must be explicitly configured and assigned an IP address. For more information, see the "Switch Virtual Interfaces" section on page 8-5 and the "Configuring Layer 3 Interfaces" section on page 8-34.

This section includes these topics:

Supported VLANs

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

Although the switch module supports a total of 1005 (normal-range and extended-range) VLANs, the number of routed ports, SVIs, and other configured features affects the use of the switch module hardware.

The switch module supports per-VLAN spanning-tree plus (PVST+) or rapid PVST+ with a maximum of 128 spanning-tree instances. One spanning-tree instance is allowed per VLAN.

Note Network node interfaces (NNIs) support STP by default. Enhanced network interfaces (ENIs) can be configured to support STP. User network interfaces (UNIs) do not support STP and by default are always in a forwarding state.

See the "VLAN Configuration Guidelines" section on page 11-8 for more information about the number of spanning-tree instances and the number of VLANs. The switch module supports IEEE 802.1Q trunking for sending VLAN traffic over Ethernet ports.

Normal-Range VLANs

Normal-range VLANs are VLANs with VLAN IDs 1 to 1005. You can add, modify or remove configurations for VLANs 2 to 1001 in the VLAN database. (VLAN IDs 1 and 1002 to 1005 are automatically created and cannot be removed.)

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

Caution You can cause inconsistency in the VLAN database if you try to manually delete the *vlan.dat* file. If you want to modify the VLAN configuration, use the commands described in these sections and in the command reference for this release.

You can set these parameters when you create a new normal-range VLAN or modify an existing VLAN in the VLAN database:

- VLAN ID
- VLAN name
- VLAN type (Ethernet, Fiber Distributed Data Interface [FDDI], FDDI network entity title [NET], TrBRF, or TrCRF, Token Ring, Token Ring-Net)

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

- VLAN state (active or suspended)
- Maximum transmission unit (MTU) for the VLAN
- Security Association Identifier (SAID)
- Bridge identification number for TrBRF VLANs
- Ring number for FDDI and TrCRF VLANs
- Parent VLAN number for TrCRF VLANs
- Spanning Tree Protocol (STP) type for TrCRF VLANs

- VLAN number to use when translating from one VLAN type to another
- Private VLAN. Configure the VLAN as a primary or secondary private VLAN. For information about private VLANs, see Chapter 12, "Private VLAN Configuration."
- Remote SPAN VLAN. Configure the VLAN as the Remote Switched Port Analyzer (RSPAN) VLAN for a remote SPAN session. For more information on remote SPAN, see Chapter 29, "Configuring SPAN and RSPAN" in the *CGS 2520 Software Configuration Guide*.
- UNI-ENI VLAN configuration

For extended-range VLANs, you can configure only MTU, private VLAN, remote SPAN VLAN, and UNI-ENI VLAN parameters.

Note This chapter does not provide configuration details for most of these parameters. For complete information on the commands and parameters that control VLAN configuration, see the command reference for this release.

Extended-Range VLANs

You can create extended-range VLANs (in the range 1006 to 4094) to enable service providers to extend their infrastructure to a greater number of customers. The extended-range VLAN IDs are allowed for any **switchport** commands that allow VLAN IDs. Extended-range VLAN configurations are not stored in the VLAN database, but they are stored in the switch module running configuration file, and you can save the configuration in the startup configuration file by using the **copy running-config startup-config** privileged EXEC command.

Note Although the switch module supports 4094 VLAN IDs, the actual number of VLANs supported is 1005.

VLAN Port Membership Modes

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

Table 11-1 Port Membership Modes

Membership Mode	VLAN Membership Characteristics
Static-access	A static-access port can belong to one VLAN and is manually assigned to that VLAN. For more information, see the "Assigning Static-Access Ports to a VLAN" section on page 11-11.
Trunk (802.1Q)	A trunk port is a member of all VLANs by default, including extended-range VLANs, but membership can be limited by configuring the allowed-VLAN list. For information about configuring trunk ports, see the "Configuring an Ethernet Interface as a Trunk Port" section on page 11-17.

Table 11-1 Port Membership Modes (continued)

Membership Mode	VLAN Membership Characteristics
Dynamic-access	A dynamic-access port can belong to one VLAN (VLAN ID 1 to 4094) and is dynamically assigned by a VMPS. The VMPS can be a Catalyst 5000 or Catalyst 6500 series switch, for example, but never a CGR 2010 ESM. The switch module is a VMPS client. **Note** Only UNIs or ENIs can be dynamic-access ports. You can have dynamic-access ports and trunk ports on the same switch module, but you must connect the dynamic-access port to an end station or hub and not to another switch module. For configuration information, see the "Configuring Dynamic-Access Ports on VMPS Clients" section on page 11-27.
Private VLAN	A private VLAN port is a host or promiscuous port that belongs to a private VLAN primary or secondary VLAN. Only NNIs can be configured as promiscuous ports. For information about private VLANs, see Chapter 12, "Configuring Private VLANs."
Tunnel (**dot1q-tunnel**)	Tunnel ports are used for 802.1Q tunneling to maintain customer VLAN integrity across a service-provider network. You configure a tunnel port on an edge switch module in the service-provider network and connect it to an 802.1Q trunk port on a customer interface, creating an assymetric link. A tunnel port belongs to a single VLAN that is dedicated to tunneling. For more information about tunnel ports, see Chapter 13, "IEEE 802.1Q and Layer 2 Protocol Tunneling Configuration."

For more detailed definitions of access and trunk modes and their functions, see Table 11-4 on page 11-16.

When a port belongs to a VLAN, the switch module learns and manages the addresses associated with the port on a per-VLAN basis.

UNI-ENI VLANs

The CGR 2010 ESM is the boundary between customer networks and the service-provider network, with user network interfaces (UNIs) and enhanced interface interfaces (ENIs) connected to the customer side of the network. When customer traffic enters or leaves the service-provider network, the customer VLAN ID must be isolated from other customers' VLAN IDs. You can achieve this isolation by several methods, including using private VLANs. On the switch module, this isolation occurs by default by using UNI-ENI VLANs.

There are two types of UNI-ENI VLANs:

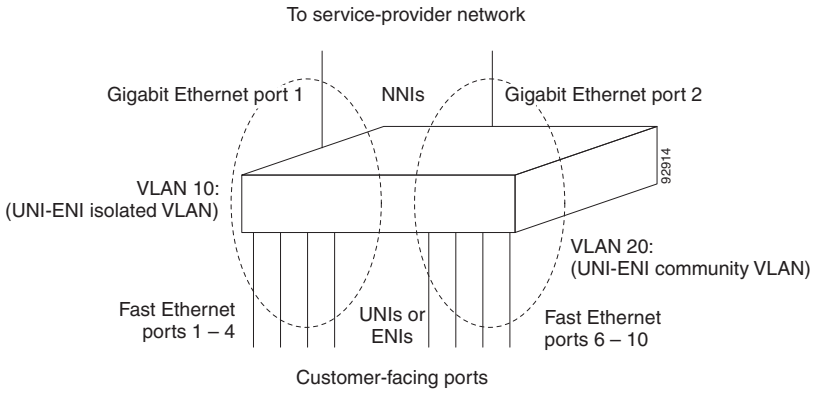
- UNI-ENI isolated VLAN—This is the default VLAN state for all VLANs created on the switch module. Local switching does not occur among UNIs or ENIs on the switch module that belong to the same UNI-ENI isolated VLAN. This configuration is designed for cases when different customers are connected to UNIs or ENIs on the same switch module. However, switching is allowed among UNIs or ENIs on different switches even though they belong to the same UNI-ENI isolated VLAN.
- UNI-ENI community VLAN—Local switching is allowed among UNIs and ENIs on the switch module that belong to the same community VLAN. If UNIs or ENIs belong to the same customer, and you want to switch module packets between the ports, you can configure the common VLAN as a UNI-ENI community VLAN. There is no local switching between the ports in a UNI-ENI community VLAN and ports outside of the VLAN. The switch module supports a combination of only eight UNIs and ENIs in a UNI-ENI community VLAN.

Note Local switching takes place between ENIs and UNIs in the same community VLAN. Because you can enable spanning tree on ENIs, but not on UNIs, you should use caution when configuring ENIs and UNIs in the same community VLAN. UNIs are always in the forwarding state.

Network node interfaces (NNIs) are not affected by the type of UNI-ENI VLAN to which they belong. Switching can occur between NNIs and other NNIs or UNIs or ENIs on the switch module or other switches that are part of the same VLAN, regardless of VLAN type.

In the configuration in Figure 11-2, if VLAN 10 is a UNI-ENI isolated VLAN and VLAN 20 is a UNI-ENI community VLAN, local switching does not take place among Fast Ethernet ports 1-4, but local switching can occur between Fast Ethernet ports 6-10. The NNIs in both VLAN 10 and VLAN 20 can exchange packets with the UNIs or ENIs in the same VLAN.

Figure 11-2 UNI -ENI Isolated and Community VLANs in the Switch Module



A UNI or ENI can be an access port, a trunk port, a private VLAN port, or an 802.1Q tunnel port. It can also be a member of an EtherChannel.

When a UNI or ENI configured as an 802.1Q trunk port belongs to a UNI-ENI isolated VLAN, the VLAN on the trunk is isolated from the same VLAN ID on a different trunk port or an access port. Other VLANs on the trunk port can be of different types (private VLAN, UNI-ENI community VLAN, and so on). For example, a UNI access port and one VLAN on a UNI trunk port can belong to the same UNI-ENI

isolated VLAN. In this case, isolation occurs between the UNI access port and the VLAN on the UNI trunk port. Other access ports and other VLANs on the trunk port are isolated because they belong to different VLANs.

UNIs, ENIs, and NNIs are always isolated from ports on different VLANs.

Creating and Modifying VLANs

You use VLAN configuration mode, accessed by entering the **vlan** global configuration command to create VLANs and to modify some parameters. You use the interface configuration mode to define the port membership mode and to add and remove ports from VLANs. The results of these commands are written to the running-configuration file, and you can display the file by entering the **show running-config** privileged EXEC command.

These sections contain VLAN configuration information:

For more efficient management of the MAC address table space available on the switch module, you can control which VLANs learn MAC addresses by disabling MAC address learning on specific VLANs. See the"Disabling MAC Address Learning on a VLAN" section on page 6-32 for more information.

Note VLAN configuration is not recommended on FastEthernet ports FE0/9 to FE0/16 on the GRWIC-D-ES-2S-8PC (Copper model) and the FastEthernet ports FE0/5 to FE0/12 on the GRWIC-D-ES-6S (SFP model). For VLAN configuration on the backplane, we recommend using Port-channel48—see Chapter 9, "EtherChannel Configuration Between the Switch Module and the Host Router."

Default Ethernet VLAN Configuration

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

Note On extended-range VLANs, you can change only the MTU size, the private VLAN, the remote SPAN, and the UNI-ENI VLAN configuration. All other characteristics must remain at the default conditions.

Table 11-2 Ethernet VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1	1 to 4094. **Note** Extended-range VLANs (VLAN IDs 1006 to 4094) are not saved in the VLAN database.
VLAN name	*VLANxxxx*, where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number	No range
802.10 SAID	100001 (100000 plus the VLAN ID)	1 to 4294967294
MTU size	1500	1500 to 9198
Translational bridge 1	0	0 to1005
Translational bridge 2	0	0 to1005
VLAN state	active	active, suspend
Remote SPAN	disabled	enabled, disabled
Private VLANs	none configured	2 to 1001, 1006 to 4094.
UNI-ENI VLAN	UNI-ENI isolated VLAN	2 to 1001, 1006 to 4094. VLAN 1 is always a UNI-ENI isolated VLAN.

VLAN Configuration Guidelines

Follow these guidelines when creating and modifying VLANs in your network:

- The switch module supports 1005 VLANs.
- Normal-range Ethernet VLANs are identified with a number between 1 and 1001. VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs.
- The switch module does not support Token Ring or FDDI media. The switch module does not forward FDDI, FDDI-Net, TrCRF, or TrBRF traffic.
- VLAN configurations for VLANs 1 to 1005 are always saved in the VLAN database and in the switch module running configuration file.
- Configuration options for VLAN IDs 1006 through 4094 (extended-range VLANs) are limited to MTU, RSPAN VLAN, private VLAN, and UNI-ENI VLAN. Extended-range VLANs are not saved in the VLAN database.
- Spanning Tree Protocol (STP) is enabled by default for only NNIs on all VLANs. You can configure STP on ENIs. NNIs and ENIs in the same VLAN are in the same spanning-tree instance. The switch module supports 128 spanning-tree instances. If a switch module has more active VLANs than supported spanning-tree instances, spanning tree can be enabled on 128 VLANs and is disabled on the remaining VLANs. If you have already used all available spanning-tree instances on a switch module, adding another VLAN creates a VLAN on that switch module that is not running spanning tree. If you have the default allowed list on the trunk ports of that switch module (which is to allow

all VLANs), the new VLAN is carried on all trunk ports. Depending on the topology of the network, this could create a loop in the new VLAN that would not be broken, particularly if there are several adjacent switches that all have run out of spanning-tree instances. You can prevent this possibility by setting allowed lists on the trunk ports of switches that have used up their allocation of spanning-tree instances.

If the number of VLANs on the switch module exceeds the number of supported spanning-tree instances, we recommend that you configure the 802.1s Multiple STP (MSTP) on your switch module to map multiple VLANs to a single spanning-tree instance.

Note MSTP is supported only on NNIs on ENIs on which STP has been enabled.

- Each routed port on the switch module creates an internal VLAN for its use. These internal VLANs use extended-range VLAN numbers, and the internal VLAN ID cannot be used for an extended-range VLAN. If you try to create an extended-range VLAN with a VLAN ID that is already allocated as an internal VLAN, an error message is generated, and the command is rejected.
  - Because internal VLAN IDs are in the lower part of the extended range, we recommend that you create extended-range VLANs beginning from the highest number (4094) and moving to the lowest (1006) to reduce the possibility of using an internal VLAN ID.
  - Before configuring extended-range VLANs, enter the **show vlan internal usage** privileged EXEC command to see which VLANs have been allocated as internal VLANs.
  - If necessary, you can shut down the routed port assigned to the internal VLAN, which frees up the internal VLAN, and then create the extended-range VLAN and re-enable the port, which then uses another VLAN as its internal VLAN. See the Creating an Extended-Range VLAN with an Internal VLAN ID, page 11-12.
- Although the switch module supports a total of 1005 (normal-range and extended-range) VLANs, the number of routed ports, SVIs, and other configured features affects the use of the switch module hardware. If you try to create an extended-range VLAN and there are not enough hardware resources available, an error message is generated, and the extended-range VLAN is rejected.

Creating or Modifying an Ethernet VLAN

To access VLAN configuration mode, enter the **vlan** global configuration command with a VLAN ID. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN. You can use the default VLAN configuration (Table 11-2) or enter commands to configure the VLAN.

Note Extended-range VLANs use the default Ethernet VLAN characteristics and the MTU, the private VLAN, the RSPAN, and the UNI-ENI VLAN configurations are the only parameters you can change.

For more information about commands available in this mode, see the **vlan** command description in the command reference for this release. When you have finished the configuration, you must exit VLAN configuration mode for the configuration to take effect. To display the VLAN configuration, enter the **show vlan** privileged EXEC command.

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

Note Before you create an extended-range VLAN, you can verify that the VLAN ID is not used internally by entering the **show vlan internal usage** privileged EXEC command. If the VLAN ID is used internally and you want to release it, go to the Creating an Extended-Range VLAN with an Internal VLAN ID, page 11-12 before creating the extended-range VLAN.

Beginning in privileged EXEC mode, follow these steps to create or modify an Ethernet VLAN:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter a VLAN ID, and enter VLAN configuration mode. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN. The available VLAN ID range for this command is 1 to 4094. **Note** When you create a new VLAN, by default the VLAN is a UNI-ENI isolated VLAN.	**vlan** *vlan-id*
Step 3	(Optional and supported on normal-range VLANs only) Enter a name for the VLAN. If no name is entered for the VLAN, the default in the VLAN database is to append the *vlan-id* with leading zeros to the word VLAN. For example, VLAN0004 is a default VLAN name for VLAN 4.	**name** *vlan-name*
Step 4	(Optional) Change the MTU size.	**mtu** *mtu-size*
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify your entries. The **name** option is only valid for VLAN IDs 1 to 1005.	**show vlan** {**name** *vlan-name* | **id** *vlan-id*}
Step 7	(Optional) Save the configuration in the switch module startup configuration file.	**copy running-config startup config**

To delete a VLAN, use the **no vlan** *vlan-id* global configuration command. You cannot delete VLAN 1 or VLANs 1002 to 1005.

Caution When you delete a VLAN, any ports assigned to that VLAN become inactive. They remain associated with the VLAN (and inactive) until you assign them to a new VLAN.

To return the VLAN name to the default settings, use the **no name** or **no mtu** VLAN configuration command.

This example shows how to create Ethernet VLAN 20, name it *test20*, and add it to the VLAN database:

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# name test20
Switch(config-vlan)# end
```

This example shows how to create a new extended-range VLAN with all default characteristics, enter config-vlan mode, and save the new VLAN in the switch module startup configuration file:

```
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config
```

Assigning Static-Access Ports to a VLAN

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

Note If you assign an interface to a VLAN that does not exist, the new VLAN is created. (See the "Creating or Modifying an Ethernet VLAN" section on page 11-9.)

Beginning in privileged EXEC mode, follow these steps to assign a port to a VLAN in the VLAN database:

	Step	Command
Step 1	Enter global configuration mode	**configure terminal**
Step 2	Enter the interface to be added to the VLAN.	**interface** *interface-id*
Step 3	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.	**no shutdown**
Step 4	Define the VLAN membership mode for the port (Layer 2 access port).	**switchport mode access**
Step 5	Assign the port to a VLAN. Valid VLAN IDs are 1 to 4094.	**switchport access vlan** *vlan-id*
Step 6	Return to privileged EXEC mode.	**end**
Step 7	Verify the VLAN membership mode of the interface.	**show running-config interface** *interface-id*
Step 8	Verify your entries in the *Administrative Mode* and the *Access Mode VLAN* fields of the display.	**show interfaces** *interface-id* **switchport**
Step 9	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To return an interface to its default configuration, use the **default interface** *interface-id* interface configuration command.

This example shows how to configure a port as an access port in VLAN 2:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# end
```

Creating an Extended-Range VLAN with an Internal VLAN ID

If you enter an extended-range VLAN ID that is already assigned to an internal VLAN, an error message appears, and the extended-range VLAN is rejected. To manually release an internal VLAN ID, you must temporarily shut down the routed port that is using the internal VLAN ID.

Beginning in privileged EXEC mode, follow these steps to release a VLAN ID that is assigned to an internal VLAN and to create an extended-range VLAN with that ID:

	Step	Command
Step 1	Display the VLAN IDs being used internally by the switch module. If the VLAN ID that you want to use is an internal VLAN, the display shows the routed port that is using the VLAN ID. Enter that port number in Step 3.	**show vlan internal usage**
Step 2	Enter global configuration mode.	**configure terminal**
Step 3	Specify the interface ID for the routed port that is using the VLAN ID, and enter interface configuration mode.	**interface** *interface-id*
Step 4	Shut down the port to release the internal VLAN ID.	**shutdown**
Step 5	Return to global configuration mode.	**exit**
Step 6	Enter the new extended-range VLAN ID, and enter config-vlan mode.	**vlan** *vlan-id*
Step 7	Exit from config-vlan mode, and return to global configuration mode.	**exit**
Step 8	Specify the interface ID for the routed port that you shut down in Step 4, and enter interface configuration mode.	**interface** *interface-id*
Step 9	Re-enable the routed port. It will be assigned a new internal VLAN ID.	**no shutdown**
Step 10	Return to privileged EXEC mode.	**end**
Step 11	(Optional) Save your entries in the switch module startup configuration file.	**copy running-config startup config**

Configuring UNI-ENI VLANs

By default, every VLAN configured on the switch module is a UNI-ENI isolated VLAN. You can change VLAN configuration to that of a UNI-ENI community VLAN, a private VLAN. or an RSPAN VLAN. You can also change the configuration of one of these VLANs to the default of a UNI-ENI isolated VLAN.

Configuration Guidelines

These are the guidelines for UNI-ENI VLAN configuration:

- UNI-ENI isolated VLANs have no effect on NNI ports.

- A UNI-ENI community VLAN is like a traditional VLAN except that it can include no more than a combination of eight UNIs and ENIs.
- To change a VLAN type, first enter the **vlan** *vlan-id* global configuration command to enter VLAN configuration mode:
  - To change a VLAN from UNI-ENI isolated VLAN to a private VLAN, enter the **private-vlan** VLAN configuration command.
  - To change a UNI-ENI community VLAN to a private VLAN, you must first remove the community VLAN type by entering the **no uni-vlan** VLAN configuration command. Then enter the **private-vlan** VLAN configuration command.
  - To change a VLAN from a UNI-ENI isolated VLAN 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. Then enter the **rspan-vlan** VLAN configuration command.
  - To change a private VLAN to a UNI-ENI VLAN, you must first remove the private VLAN type by entering the **no private-vlan** VLAN configuration command. Then enter the **uni-vlan** VLAN configuration command.
  - To change an RSPAN VLAN to a UNI-ENI VLAN, you must first remove the RSPAN VLAN type by entering the **no rspan-vlan** VLAN configuration command. Then enter the **uni-vlan** VLAN configuration command
- The switch module supports a total of eight UNIs and ENIs in a community VLAN. You cannot configure a VLAN as a UNI-ENI community VLAN if more than eight UNIs and ENIs belong to the VLAN.
- If you attempt to add a UNI or ENI static access port to a UNI-ENI community VLAN that has a combination of eight UNIs and ENIs, the configuration is refused. If a UNI or ENI dynamic access port is added to a UNI-ENI community VLAN that has eight UNIs or ENIs, the port is error-disabled.
- Use caution when configuring ENIs and UNIs in the same community VLAN. Local switching takes place between the ENIs and UNIs in the community VLAN and ENIs can support spanning tree while UNIs do not.

Configuring UNI-ENI VLANs

By default, every VLAN created on the switch module is a UNI-ENI isolated VLAN. You can change the configuration to UNI-ENI community VLAN or to a private VLAN or RSPAN VLAN. For procedures for configuring private VLANs, see Chapter 12, “Private VLAN Configuration.”

Beginning in privileged EXEC mode, follow these steps to change the type of a UNI-ENI VLAN:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter a VLAN ID, and enter VLAN configuration mode. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN. By default, the VLAN is a UNI-ENI isolated VLAN. **Note** The available VLAN ID range for this command is 1 to 4094.	**vlan** *vlan-id*
Step 3	Configure the UNI-ENI VLAN type. • Enter **community** to change from the default to a UNI-ENI community VLAN. • Enter **isolated** to return to the default UNI-ENI isolated VLAN. **Note** VLAN 1 is always a UNI-ENI isolated VLAN; you cannot configure VLAN 1 as a UNI-ENI community VLAN. The reserved VLANs 1002 to 1005 are not Ethernet VLANs.	**uni-vlan** {**community** | **isolated**}
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Display UNI-ENI VLAN information. Enter **type** (optional) to see only the VLAN ID and type of UNI-ENI VLAN.	**show vlan uni-vlan** [**type**]
Step 6	(Optional) Save the configuration in the switch module startup configuration file.	**copy running-config startup config**

Use the **no uni-vlan** VLAN configuration command to return to the default (UNI-ENI isolated VLAN). Entering **uni-vlan isolated** command has the same effect as entering the no **uni-vlan** VLAN configuration command. The **show vlan** and **show vlan** *vlan-id* privileged EXEC commands also display UNI-ENI VLAN information, but only UNI-ENI community VLANs appear. To display both isolated and community VLANs, use the **show vlan uni-vlan type** command.

Displaying VLANs

Use the **show vlan** privileged EXEC command to display a list of all VLANs on the switch module, including extended-range VLANs. The display includes VLAN status, ports, and configuration information. Table 11-3 lists other privileged EXEC commands for monitoring VLANs.

Table 11-3 VLAN Monitoring Commands

Command	Description
show interfaces [**vlan** *vlan-id*]	Display characteristics for all interfaces or for the specified VLAN configured on the switch module.
show vlan [**id** *vlan-id*]	Display parameters for all VLANs or the specified VLAN on the switch module.
show vlan [*vlan-name*] **uni-vlan type**	Display UNI-ENI isolated or UNI-ENI community VLANs by VLAN name.
show vlan uni-vlan	Display UNI-ENI community VLANs and associated ports on the switch module.
show vlan uni-vlan type	Display UNI-ENI isolated and UNI-ENI community VLANs on the switch module by VLAN ID.

For more details about the **show** command options and explanations of output fields, see the command reference for this release.

Configuring VLAN Trunks

Trunking Overview

A trunk is a point-to-point link between one or more Ethernet switch module interfaces and another networking device such as a router or a switch module. Ethernet trunks carry the traffic of multiple VLANs over a single link, and you can extend the VLANs across an entire network. The switch module supports the 802.1Q industry-standard trunking encapsulation.

You can configure a trunk on a single Ethernet interface or on an EtherChannel bundle.

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

- If you do not intend to trunk across links, use the **switchport mode access** interface configuration command to disable trunking.

- To enable trunking, use the **switchport mode trunk** interface configuration command to change the interface to a trunk.

Table 11-4 Layer 2 Interface Modes

Mode	Function
switchport mode access	Puts the interface (access port) into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes a nontrunk interface regardless of whether or not the neighboring interface is a trunk interface. This is the default mode.
switchport mode trunk	Puts the interface into permanent trunking mode and negotiates to convert the neighboring link into a trunk link. The interface becomes a trunk interface even if the neighboring interface is not a trunk interface.
switchport mode dot1q-tunnel	Configures the interface as a tunnel (nontrunking) port to be connected in an asymmetric link with an 802.1Q trunk port. The 802.1Q tunneling is used to maintain customer VLAN integrity across a service provider network. See Chapter 13, "Configuring IEEE 802.1Q Tunneling," for more information on tunnel ports.
switchport mode private-vlan	Configure the interface as a private VLAN host or promiscuous port (only NNIs can be configured as promiscuous ports). For information about private VLANs, see Chapter 12, "Configuring Private VLANs."

IEEE 802.1Q Configuration Considerations

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

- In a network of Cisco switches connected through 802.1Q trunks, the switches maintain one spanning-tree instance for each VLAN allowed on the trunks. Non-Cisco devices might support one spanning-tree instance for all VLANs.

  When you connect a Cisco switch module to a non-Cisco device through an 802.1Q trunk, the Cisco switch module combines the spanning-tree instance of the VLAN of the trunk with the spanning-tree instance of the non-Cisco 802.1Q switch module. However, spanning-tree information for each VLAN is maintained by Cisco switches separated by a cloud of non-Cisco 802.1Q switches. The non-Cisco 802.1Q cloud separating the Cisco switches is treated as a single trunk link between the switches.

- Make sure that the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning-tree loops might result.

- Disabling spanning tree on the native VLAN of an 802.1Q trunk without disabling spanning tree on every VLAN in the network can potentially cause spanning-tree loops. We recommend that you leave spanning tree enabled on the native VLAN of an 802.1Q trunk or disable spanning tree on every VLAN in the network. Make sure that your network is loop-free before disabling spanning tree.

Default Layer 2 Ethernet Interface VLAN Configuration

Table 11-5 shows the default Layer 2 Ethernet interface VLAN configuration.

Table 11-5 Default Layer 2 Ethernet Interface VLAN Configuration

Feature	Default Setting
Interface mode	**switchport mode access**
Allowed VLAN range	VLANs 1 to 4094
Default VLAN (for access ports)	VLAN 1
Native VLAN (for 802.1Q trunks)	VLAN 1

Configuring an Ethernet Interface as a Trunk Port

Interaction with Other Features

Trunking interacts with other features in these ways:

- A trunk port cannot be a secure port
- A trunk port cannot be a tunnel port
- Trunk ports can be grouped into EtherChannel port groups, but all trunks in the group must have the same configuration. When a group is first created, all ports follow the parameters set for the first port to be added to the group. If you change the configuration of one of these parameters, the switch module propagates the setting that you entered to all ports in the group:
  - allowed-VLAN list
  - STP port priority for each VLAN
  - STP Port Fast setting

Note STP is supported by default on NNIs, but must be enabled on ENIs. STP is not supported on UNIs.

  - trunk status: if one port in a port group ceases to be a trunk, all ports cease to be trunks.
- If you try to enable 802.1x on a trunk port, an error message appears, and 802.1x is not enabled. If you try to change the mode of an 802.1x-enabled port to trunk, the port mode is not changed.

Configuring a Trunk Port

- Beginning in privileged EXEC mode, follow these steps to configure a port as an 802.1Q trunk port:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the port to be configured for trunking, and enter interface configuration mode.	**interface** *interface-id*
Step 3	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.	**no shutdown**
Step 4	Configure the interface as a Layer 2 trunk.	**switchport mode trunk**
Step 5	(Optional) Specify the default VLAN, which is used if the interface stops trunking.	**switchport access vlan** *vlan-id*
Step 6	Specify the native VLAN for 802.1Q trunks.	**switchport trunk native vlan** *vlan-id*
Step 7	Return to privileged EXEC mode.	**end**
Step 8	Display the switchport configuration of the interface in the *Administrative Mode* field of the display.	**show interfaces** *interface-id* **switchport**
Step 9	Display the trunk configuration of the interface.	**show interfaces** *interface-id* **trunk**
Step 10	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To return an interface to its default configuration, use the **default interface** *interface-id* interface configuration command. To reset all trunking characteristics of a trunking interface to the defaults, use the **no switchport trunk** interface configuration command. To disable trunking, use the **switchport mode access** interface configuration command to configure the port as a static-access port.

This example shows how to configure a port as an 802.1Q trunk with VLAN 33 as the native VLAN:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 33
Switch(config-if)# end
```

Defining the Allowed VLANs on a Trunk

By default, a trunk port sends traffic to and receives traffic from all VLANs. All VLAN IDs, 1 to 4094, are allowed on each trunk. However, you can remove VLANs from the allowed list, preventing traffic from those VLANs from passing over the trunk. To restrict the traffic a trunk carries, use the **switchport trunk allowed vlan remove** *vlan-list* interface configuration command to remove specific VLANs from the allowed list.

Note VLAN 1 is the default VLAN on all trunk ports in all Cisco switches, and it has previously been a requirement that VLAN 1 always be enabled on every trunk link. The VLAN 1 minimization feature allows you to disable VLAN 1 on any individual VLAN trunk link so that no user traffic (including spanning-tree advertisements) is sent or received on VLAN 1. You do this by removing VLAN 1 from the allowed VLAN list.

To reduce the risk of spanning-tree loops or storms, you can disable VLAN 1 on any individual VLAN trunk port by removing VLAN 1 from the allowed list. When you remove VLAN 1 from a trunk port, the interface continues to send and receive management traffic, for example, Cisco Discovery Protocol (CDP), and Link Aggregation Control Protocol (LACP) in VLAN 1.

If a trunk port with VLAN 1 disabled is converted to a nontrunk port, it is added to the access VLAN. If the access VLAN is set to 1, the port is added to VLAN 1, regardless of the **switchport trunk allowed** setting. The same is true for any VLAN that has been disabled on the port.

A trunk port can become a member of a VLAN if the VLAN is enabled and if the VLAN is in the allowed list for the port.

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

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the port to be configured, and enter interface configuration mode.	**interface** *interface-id*
Step 3	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.	**no shutdown**
Step 4	Configure the interface as a VLAN trunk port.	**switchport mode trunk**
Step 5	(Optional) Configure the list of VLANs allowed on the trunk. For explanations about using the **add**, **all**, **except**, and **remove** keywords, see the command reference for this release. The *vlan-list* parameter is either a single VLAN number from 1 to 4094 or a range of VLANs described by two VLAN numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated VLAN parameters or in hyphen-specified ranges. All VLANs are allowed by default.	**switchport trunk allowed vlan** {**add** | **all** | **except** | **remove**} *vlan-list*
Step 6	Return to privileged EXEC mode.	**end**
Step 7	Verify your entries in the *Trunking VLANs Enabled* field of the display.	**show interfaces** *interface-id* **switchport**
Step 8	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To return to the default allowed VLAN list of all VLANs, use the **no switchport trunk allowed vlan** interface configuration command.

This example shows how to remove VLAN 2 from the allowed VLAN list on a port:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport trunk allowed vlan remove 2
Switch(config-if)# end
```

Configuring the Native VLAN for Untagged Traffic

A trunk port configured with 802.1Q tagging can receive both tagged and untagged traffic. By default, the switch module forwards untagged traffic in the native VLAN configured for the port. The native VLAN is VLAN 1 by default.

Note The native VLAN can be assigned any VLAN ID.

For information about 802.1Q configuration issues, see the "IEEE 802.1Q Configuration Considerations" section on page 11-16.

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

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Define the interface that is configured as the 802.1Q trunk, and enter interface configuration mode.	**interface** *interface-id*
Step 3	Enable the port, if necessary. By default, UNIs and ENIs are disabled and NNIs are enabled.	**no shutdown**
Step 4	Configure the VLAN that is sending and receiving untagged traffic on the trunk port. For *vlan-id*, the range is 1 to 4094.	**switchport trunk native vlan** *vlan-id*
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify your entries in the *Trunking Native Mode VLAN* field.	**show interfaces** *interface-id* **switchport**
Step 7	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To return to the default native VLAN, VLAN 1, use the **no switchport trunk native vlan** interface configuration command.

If a packet has a VLAN ID that is the same as the sending port native VLAN ID, the packet is sent untagged; otherwise, the switch module sends the packet with a tag.

Configuring Trunk Ports for Load Sharing

Load sharing divides the bandwidth supplied by parallel trunks that connect switches. To avoid loops, STP normally blocks all but one parallel link between switches. Using load sharing, you divide the traffic between the links according to the VLAN to which the traffic belongs.

You configure load sharing on trunk ports that have STP enabled by using STP port priorities or STP path costs. For load sharing using STP port priorities, both load-sharing links must be connected to the same switch module. For load sharing using STP path costs, each load-sharing link can be connected to the same switch module or to two different switch modules.

Load Sharing Using STP Port Priorities

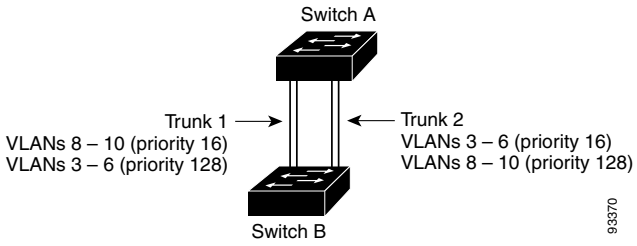
When two ports on the same switch module form a loop, the switch module uses the STP port priority to decide which port is enabled and which port is in a blocking state. You can set the priorities on a parallel STP trunk port so that the port carries all the traffic for a given VLAN. The trunk port with the higher priority (lower values) for a VLAN is forwarding traffic for that VLAN. The trunk port with the lower priority (higher values) for the same VLAN remains in a blocking state for that VLAN. One trunk port sends or receives all traffic for the VLAN.

Figure 11-3 shows two trunks connecting supported switches. In this example, the switches are configured as follows:

- VLANs 8 through 10 are assigned a port priority of 16 on Trunk 1
- VLANs 3 through 6 retain the default port priority of 128 on Trunk 1
- VLANs 3 through 6 are assigned a port priority of 16 on Trunk 2
- VLANs 8 through 10 retain the default port priority of 128 on Trunk 2

In this way, Trunk 1 carries traffic for VLANs 8 through 10, and Trunk 2 carries traffic for VLANs 3 through 6. If the active trunk fails, the trunk with the lower priority takes over and carries the traffic for all of the VLANs. No duplication of traffic occurs over any trunk port.

Figure 11-3 Load Sharing by Using STP Port Priorities



Beginning in privileged EXEC mode on Switch A, follow these steps to configure the network shown in Figure 11-3. Note that you can use any interface numbers; those shown are examples only.

	Step	Command
Step 1	Verify that the referenced VLANs exist on Switch A. If not, create the VLANs by entering the VLAN IDs.	**show vlan**
Step 2	Enter global configuration mode.	**configure terminal**

	Step	Command
Step 3	Define the interface to be configured as the Trunk 1 interface, and enter interface configuration mode.	**interface gigabitethernet 0/1**
Step 4	Configure the interface as an NNI or ENI. UNIs do not support STP. If you configure the port as an ENI, you must also enable STP on the port by entering the **spanning-tree** interface configuration command.	**port-type** {**nni** | **eni**}
Step 5	Configure the port as a trunk port.	**switchport mode trunk**
Step 6	Assign the port priority of 16 for VLANs 8 through 10 on Trunk 1.	**spanning-tree vlan 8-10 port-priority 16**
Step 7	Return to privileged EXEC mode.	**end**
Step 8	Verify the port configuration.	**show interfaces gigabitethernet 0/1 switchport**
Step 9	Enter global configuration mode.	**configure terminal**
Step 10	Define the interface to be configured as the Trunk 2 interface, and enter interface configuration mode.	**interface gigabitethernet 0/2**
Step 11	Configure the interface as an NNI or ENI. UNIs do not support STP. If you configure the port as an ENI, you must also enable STP on the port by entering the **spanning-tree** interface configuration command.	**port-type** {**nni** | **eni**}
Step 12	Configure the port as a trunk port.	**switchport mode trunk**
Step 13	Assign the port priority of 16 for VLANs 3 through 6 on Trunk 2.	**spanning-tree vlan 3-6 port-priority 16**
Step 14	Return to privileged EXEC mode.	**end**
Step 15	Verify the port configuration.	**show interfaces gigabitethernet 0/2 switchport**
Step 16	Verify your entries.	**show running-config**
Step 17	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

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

Load Sharing Using STP Path Cost

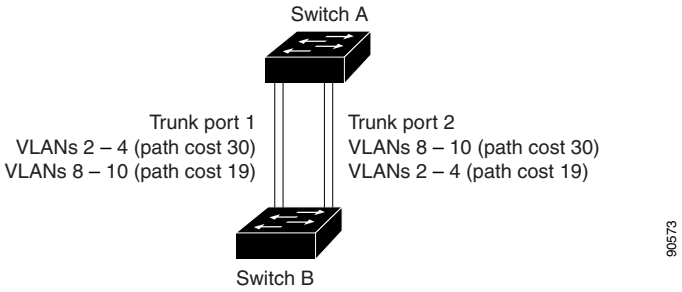
You can configure parallel trunks to share VLAN traffic by setting different path costs on a trunk and associating the path costs with different sets of VLANs, blocking different ports for different VLANs. The VLANs keep the traffic separate and maintain redundancy in the event of a lost link.

In Figure 11-4, Trunk ports 1 and 2 are configured as 100Base-T ports. These VLAN path costs are assigned:

- VLANs 2 through 4 are assigned a path cost of 30 on Trunk port 1

- VLANs 8 through 10 retain the default 100Base-T path cost on Trunk port 1 of 19
- VLANs 8 through 10 are assigned a path cost of 30 on Trunk port 2
- VLANs 2 through 4 retain the default 100Base-T path cost on Trunk port 2 of 19

Figure 11-4 Load-Sharing Trunks with Traffic Distributed by Path Cost



Beginning in privileged EXEC mode, follow these steps to configure the network shown in Figure 11-4:

	Step	Command
Step 1	Enter global configuration mode on Switch A.	**configure terminal**
Step 2	Define the interface to be configured as Trunk port 1, and enter interface configuration mode.	**interface fastethernet0/1**
Step 3	Configure the interface as an NNI or ENI. UNIs do not support STP. If you configure the port as an ENI, you must also enable STP on the port by entering the **spanning-tree** interface configuration command.	**port-type** {**nni** | **eni**}
Step 4	Configure the port as a trunk port.	**switchport mode trunk**
Step 5	Return to global configuration mode.	**exit**
Step 6	Define the interface to be configured as Trunk port 2, and enter interface configuration mode.	**interface fastethernet0/2**
Step 7	Configure the interface as an NNI or ENI. UNIs do not support STP. If you configure the port as an ENI, you must also enable STP on the port by entering the **spanning-tree** interface configuration command.	**port-type** {**nni** | **eni**}
Step 8	Configure the port as a trunk port.	**switchport mode trunk**
Step 9	Return to privileged EXEC mode.	**end**
Step 10	Verify your entries. In the display, make sure that the interfaces configured in Steps 2 and 7 are configured as trunk ports.	**show running-config**
Step 11	Verify that VLANs 2 through 4 and 8 through 10 are configured on Switch A. If not, create these VLANs.	**show vlan**
Step 12	Enter global configuration mode.	**configure terminal**
Step 13	Enter interface configuration mode for Trunk port 2.	**interface fastethernet0/1**

	Step	Command
Step 14	Set the spanning-tree path cost to 30 for VLANs 2 through 4.	**spanning-tree vlan 2-4 cost 30**
Step 15	Return to global configuration mode.	**exit**
Step 16	Enter interface configuration mode for Trunk port 2.	**interface fastethernet0/2**
Step 17	Set the spanning-tree path cost to 30 for VLANs 2 through 4.	**spanning-tree vlan 8-10 cost 30**
Step 18	Return to global configuration mode.	**exit**
Step 19	Repeat Steps 9 through 11 on the other configured trunk interface on Switch A, and set the spanning-tree path cost to 30 for VLANs 8, 9, and 10.	
Step 20	Return to privileged EXEC mode.	**exit**
Step 21	Verify your entries. In the display, verify that the path costs are set correctly for both trunk interfaces.	**show running-config**
Step 22	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

Follow the same steps on Switch B to configure the trunk port for Trunk 1 with a path cost of 30 for VLANs 2 through 4, and configure the trunk port for Trunk 2 with a path cost of 30 for VLANs 8 through 10.

Configuring VMPS

The VLAN Query Protocol (VQP) supports dynamic-access ports, which are not permanently assigned to a VLAN, but give VLAN assignments based on the MAC source addresses seen on the port.

Note Only UNIs and ENIs can be configured as dynamic-access ports; NNIs cannot take part in VQP.

Each time an unknown MAC address is seen, the switch module sends a VQP query to a remote VMPS; the query includes the newly seen MAC address and the port on which it was seen. The VMPS responds with a VLAN assignment for the port. The switch module cannot be a VMPS server but can act as a client to the VMPS and communicate with it through VQP.

Understanding VMPS

Each time the client switch module receives the MAC address of a new host, it sends a VQP query to the VMPS. When the VMPS receives this query, it searches its database for a MAC-address-to-VLAN mapping. The server response is based on this mapping and whether or not the server is in open or secure mode. In secure mode, the server shuts down the port when an illegal host is detected. In open mode, the server simply denies the host access to the port.

If the port is currently *unassigned* (that is, it does not yet have a VLAN assignment), the VMPS provides one of these responses:

- If the host is allowed on the port, the VMPS sends the client a *vlan-assignment* response containing the assigned VLAN name and allowing access to the host.
- If the host is not allowed on the port and the VMPS is in open mode, the VMPS sends an *access-denied* response.
- If the VLAN is not allowed on the port and the VMPS is in secure mode, the VMPS sends a *port-shutdown* response.

If the port already has a VLAN assignment, the VMPS provides one of these responses:

- If the VLAN in the database matches the current VLAN on the port, the VMPS sends an *success* response, allowing access to the host.
- If the VLAN in the database does not match the current VLAN on the port and active hosts exist on the port, the VMPS sends an *access-denied* or a *port-shutdown* response, depending on the secure mode of the VMPS.

If the switch module receives an *access-denied* response from the VMPS, it continues to block traffic to and from the host MAC address. The switch module continues to monitor the packets directed to the port and sends a query to the VMPS when it identifies a new host address. If the switch module receives a *port-shutdown* response from the VMPS, it disables the port. The port must be manually re-enabled by using the CLI or SNMP.

Dynamic-Access Port VLAN Membership

A dynamic-access port can belong to only one VLAN with an ID from 1 to 4094. When the link comes up, the switch module does not forward traffic to or from this port until the VMPS provides the VLAN assignment. The VMPS receives the source MAC address from the first packet of a new host connected to the dynamic-access port and attempts to match the MAC address to a VLAN in the VMPS database.

Note Only UNIs or ENIs can be dynamic-access ports.

If there is a match, the VMPS sends the VLAN number for that port. If the client switch module was not previously configured, it uses the domain name from the first VTP packet it receives on its trunk port from the VMPS. If the client switch module was previously configured, it includes its domain name in the query packet to the VMPS to obtain its VLAN number. The VMPS verifies that the domain name in the packet matches its own domain name before accepting the request and responds to the client with the assigned VLAN number for the client. If there is no match, the VMPS either denies the request or shuts down the port (depending on the VMPS secure mode setting).

Multiple hosts (MAC addresses) can be active on a dynamic-access port if they are all in the same VLAN; however, the VMPS shuts down a dynamic-access port if more than 20 hosts are active on the port.

If the link goes down on a dynamic-access port, the port returns to an isolated state and does not belong to a VLAN. Any hosts that come online through the port are checked again through the VQP with the VMPS before the port is assigned to a VLAN.

Dynamic-access ports can be used for direct host connections, or they can connect to a network. A maximum of 20 MAC addresses are allowed per port on the switch module. A dynamic-access port can belong to only one VLAN at a time, but the VLAN can change over time, depending on the MAC addresses seen.

Default VMPS Client Configuration

Table 11-6 shows the default VMPS and dynamic-access port configuration on client switches.

Table 11-6 Default VMPS Client and Dynamic-Access Port Configuration

Feature	Default Setting
VMPS domain server	None
VMPS reconfirm interval	60 minutes
VMPS server retry count	3
Dynamic-access ports	None configured

VMPS Configuration Guidelines

These guidelines and restrictions apply to dynamic-access port VLAN membership:

- You should configure the VMPS before you configure ports as dynamic-access ports.
- 802.1x ports cannot be configured as dynamic-access ports. If you try to enable 802.1x on a dynamic-access (VQP) port, an error message appears, and 802.1x is not enabled. If you try to change an 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.
- Trunk ports cannot be dynamic-access ports, but you can enter the **switchport access vlan dynamic** interface configuration command for a trunk port. In this case, the switch module retains the setting and applies it if the port is later configured as an access port.

  You must turn off trunking on the port before the dynamic-access setting takes effect.
- Dynamic-access ports cannot be monitor ports.
- Secure ports cannot be dynamic-access ports. You must disable port security on a port before it becomes dynamic.
- Private VLAN ports cannot be dynamic-access ports.
- Dynamic-access ports cannot be members of an EtherChannel group.
- Port channels cannot be configured as dynamic-access ports.

Configuring the VMPS Client

You configure dynamic VLANs by using the VMPS (server). The switch module can be a VMPS client; it cannot be a VMPS server.

Entering the IP Address of the VMPS

You must first enter the IP address of the server to configure the switch module as a client.

Beginning in privileged EXEC mode, follow these steps to enter the IP address of the VMPS:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter the IP address of the switch module acting as the primary VMPS server.	**vmps server** *ipaddress* **primary**
Step 3	(Optional) Enter the IP address of the switch module acting as a secondary VMPS server. You can enter up to three secondary server addresses.	**vmps server** *ipaddress*
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entries in the *VMPS Domain Server* field of the display.	**show vmps**
Step 6	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

Note You must have IP connectivity to the VMPS for dynamic-access ports to work. You can test for IP connectivity by pinging the IP address of the VMPS and verifying that you get a response.

Configuring Dynamic-Access Ports on VMPS Clients

Caution Dynamic-access port VLAN membership is for end stations or hubs connected to end stations. Connecting dynamic-access ports to other switch modules can cause a loss of connectivity.

Beginning in privileged EXEC mode, follow these steps to configure a dynamic-access port on a VMPS client switch module:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the switch module port that is connected to the end station, and enter interface configuration mode. The port must be a UNI or an ENI.	**interface** *interface-id*
Step 3	Enable the port.	**no shutdown**
Step 4	Configure the port as a UNI or ENI.	**port-type** {**uni** | **eni**}
Step 5	Set the port to access mode.	**switchport mode access**

	Step	Command
Step 6	Configure the port as eligible for dynamic VLAN membership. The dynamic-access port must be connected to an end station.	**switchport access vlan dynamic**
Step 7	Return to privileged EXEC mode.	**end**
Step 8	Verify your entries in the *Operational Mode* field of the display.	**show interfaces** *interface-id* **switchport**
Step 9	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To return an interface to its default configuration, use the **default interface** *interface-id* interface configuration command. To reset the access mode to the default VLAN for the switch module, use the **no switchport access vlan** interface configuration command.

Reconfirming VLAN Memberships

Beginning in privileged EXEC mode, follow these steps to confirm the dynamic-access port VLAN membership assignments that the switch module has received from the VMPS:

	Step	Command
Step 1	Reconfirm dynamic-access port VLAN membership.	**vmps reconfirm**
Step 2	Verify the dynamic VLAN reconfirmation status.	**show vmps**

Changing the Reconfirmation Interval

VMPS clients periodically reconfirm the VLAN membership information received from the VMPS.You can set the number of minutes after which reconfirmation occurs.

Beginning in privileged EXEC mode, follow these steps to change the reconfirmation interval:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter the number of minutes between reconfirmations of the dynamic VLAN membership. The range is 1 to 120. The default is 60 minutes.	**vmps reconfirm** *minutes*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify the dynamic VLAN reconfirmation status in the *Reconfirm Interval* field of the display.	**show vmps**
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To return the switch module to its default setting, use the **no vmps reconfirm** global configuration command.

Changing the Retry Count

Beginning in privileged EXEC mode, follow these steps to change the number of times that the switch module attempts to contact the VMPS before querying the next server:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Change the retry count. The retry range is 1 to 10; the default is 3.	**vmps retry** *count*
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entry in the *Server Retry Count* field of the display.	**show vmps**
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To return the switch module to its default setting, use the **no vmps retry** global configuration command.

Monitoring the VMPS

You can display information about the VMPS by using the **show vmps** privileged EXEC command. The switch module displays this information about the VMPS:

- VMPS VQP Version—the version of VQP used to communicate with the VMPS. The switch module queries the VMPS that is using VQP Version 1.
- Reconfirm Interval—the number of minutes the switch module waits before reconfirming the VLAN-to-MAC-address assignments.
- Server Retry Count—the number of times VQP resends a query to the VMPS. If no response is received after this many tries, the switch module starts to query the secondary VMPS.
- VMPS domain server—the IP address of the configured VLAN membership policy servers. The switch module sends queries to the one marked *current*. The one marked *primary* is the primary server.
- VMPS Action—the result of the most recent reconfirmation attempt. A reconfirmation attempt can occur automatically when the reconfirmation interval expired, or you can force it by entering the **vmps reconfirm** privileged EXEC command.

This is an example of output for the **show vmps** privileged EXEC command:

```
Switch# show vmps
VQP Client Status:
--------------------
VMPS VQP Version:   1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.128.86 (primary, current)
```

```
                    172.20.128.87
Reconfirmation status
---------------------
VMPS Action:         other
```

Troubleshooting Dynamic-Access Port VLAN Membership

The VMPS shuts down a dynamic-access port under these conditions:

- The VMPS is in secure mode, and it does not allow the host to connect to the port. The VMPS shuts down the port to prevent the host from connecting to the network.
- More than 20 active hosts reside on a dynamic-access port

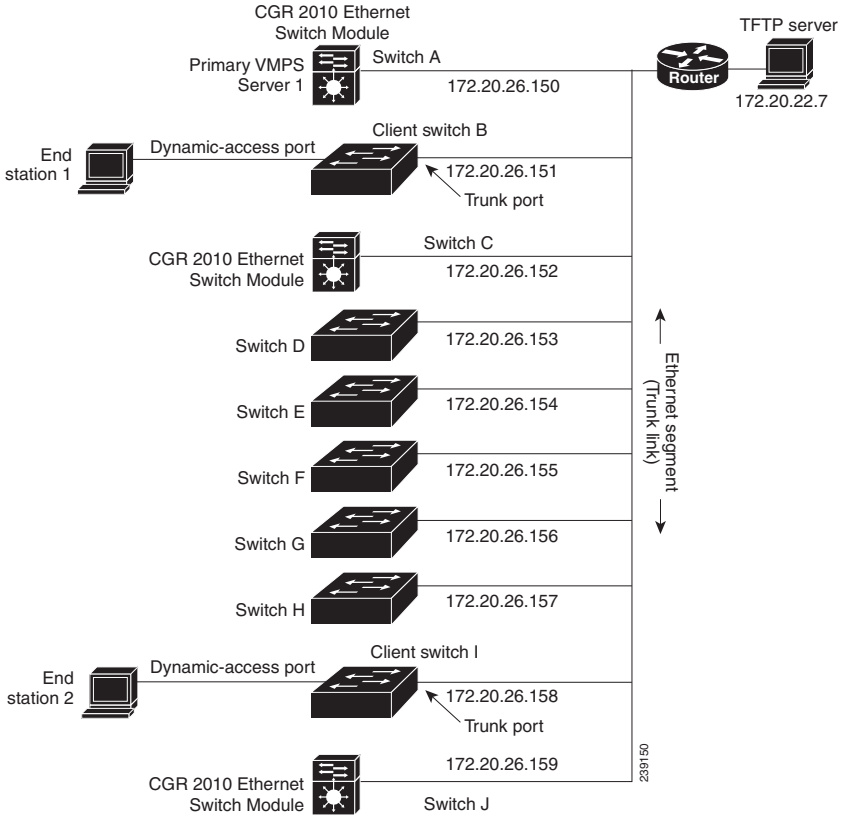
To disable and re-enable a disabled dynamic-access port, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.

VMPS Configuration Example

Figure 11-5 shows a network with a VMPS server switch module and VMPS client switch module with dynamic-access ports. In this example, these assumptions apply:

- The VMPS server and the VMPS client are separate switches
- The CGR 2010 ESM (Switch A) is the primary VMPS server
- The CGR 2010 ESM Switch C and Switch J are secondary VMPS servers
- End stations are connected to the clients, Switch B and Switch I
- The database configuration file is stored on the TFTP server with the IP address 172.20.22.7

Figure 11-5 Dynamic Port VLAN Membership Configuration



Private VLAN Configuration

This chapter describes how to configure private VLANs on the CGR 2010 ESM.

Note For complete syntax and usage information for the commands used in this chapter, see the online *Cisco IOS Interface Command Reference, Release 12.2*.

Understanding Private VLANs

The private-VLAN feature addresses two problems that service providers face when using VLANs:

- Scalability: The switch module supports up to 1,005 active VLANs. If a service provider assigns one VLAN per customer, this limits the numbers of customers that the service provider can support.
- To enable IP routing, each VLAN is assigned a subnet address space or a block of addresses, which can waste the unused IP addresses and cause IP address management problems.

Using private VLANs addresses the scalability problem and provides IP address management benefits for service providers and Layer 2 security for customers.

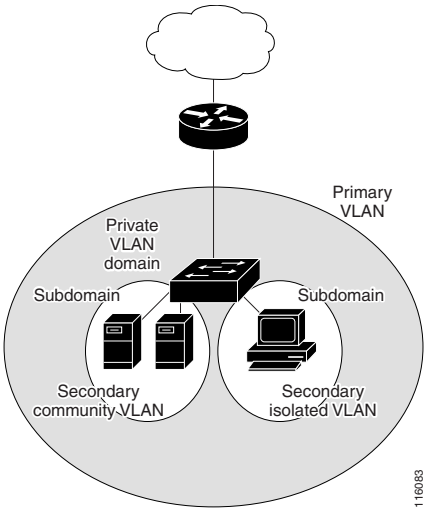
These sections describe how private VLANs work:

Types of Private VLANs and Private-VLAN Ports

Private VLANs partition a regular VLAN domain into subdomains. A subdomain is represented by a pair of VLANs: a *primary* VLAN and a *secondary* VLAN. A private VLAN can have multiple VLAN pairs, one pair for each subdomain. All VLAN pairs in a private VLAN share the same primary VLAN. The

secondary VLAN ID differentiates one subdomain from another. See Figure 12-1.

Figure 12-1 Private-VLAN Domain



There are two types of secondary VLANs:

- Isolated VLANs—Ports within an isolated VLAN cannot communicate with each other at the Layer 2 level.
- Community VLANs—Ports within a community VLAN can communicate with each other but cannot communicate with ports in other communities at the Layer 2 level. A community VLAN can include a combination of no more than eight user network interfaces (UNIs) and enhanced network interfaces (ENIs).

Private VLANs provide Layer 2 isolation between ports within the same private VLAN. Private-VLAN ports are access ports that are one of these types:

- Promiscuous—A promiscuous port belongs to the primary VLAN and can communicate with all interfaces, including the community and isolated host ports that belong to the secondary VLANs associated with the primary VLAN.

Note Promiscuous ports must be network node interfaces (NNIs). UNIs or ENIs cannot be configured as promiscuous ports.

- Isolated—An isolated port is a host port that belongs to an isolated secondary VLAN. It has complete Layer 2 separation from other ports within the same private VLAN, except for the promiscuous ports. Private VLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports.
- Community—A community port is a host port that belongs to a community secondary VLAN. Community ports communicate with other ports in the same community VLAN and with promiscuous ports. These interfaces are isolated at Layer 2 from all other interfaces in other communities and from isolated ports within their private VLAN. No more than eight UNIs and ENIs can be community ports in the same community VLAN.

Note Trunk ports carry traffic from regular VLANs and also from primary, isolated, and community VLANs.

Primary and secondary VLANs have these characteristics:

- Primary VLAN—A private VLAN has only one primary VLAN. Every port in a private VLAN is a member of the primary VLAN. The primary VLAN carries unidirectional traffic downstream from the promiscuous ports to the (isolated and community) host ports and to other promiscuous ports.
- Isolated VLAN —A private VLAN has only one isolated VLAN. An isolated VLAN is a secondary VLAN that carries unidirectional traffic upstream from the hosts toward the promiscuous ports and the gateway.
- Community VLAN—A community VLAN is a secondary VLAN that carries upstream traffic from the community ports to the promiscuous port gateways and to other host ports in the same community. You can configure multiple community VLANs in a private VLAN. Each community VLAN can include a combination of no more than eight UNIs and ENIs.

Note The switch module also supports UNI-ENI isolated VLANs and UNI-ENI community VLANs. When a VLAN is created, it is by default a UNI-ENI isolated VLAN. Traffic is not switched among UNIs and ENIs on a switch module that belong to a UNI-ENI isolated VLAN. For more information on UNI-ENI VLANs, see Chapter 11, "VLAN Configuration."

A promiscuous port can serve only one primary VLAN, one isolated VLAN, and multiple community VLANs. Layer 3 gateways are typically connected to the switch module through a promiscuous port. With a promiscuous port, you can connect a wide range of devices as access points to a private VLAN. For example, you can use a promiscuous port to monitor or back up all the private-VLAN servers from an administration workstation.

In a switched environment, you can assign an individual private VLAN and associated IP subnet to each individual or common group of end stations. The end stations need to communicate only with a default gateway to communicate outside the private VLAN.

You can use private VLANs to control access to end stations in these ways:

- Configure selected interfaces connected to end stations as isolated ports to prevent any communication at Layer 2. For example, if the end stations are servers, this configuration prevents Layer 2 communication between the servers.
- Configure NNIs connected to default gateways and selected end stations (for example, backup servers) as promiscuous ports to allow all end stations access to a default gateway.

You can extend private VLANs across multiple devices by trunking the primary, isolated, and community VLANs to other devices that support private VLANs. To maintain the security of your private-VLAN configuration and to avoid other use of the VLANs configured as private VLANs, configure private VLANs on all intermediate devices, including devices that have no private-VLAN ports.

IP Addressing Scheme with Private VLANs

Assigning a separate VLAN to each customer creates an inefficient IP addressing scheme:

- Assigning a block of addresses to a customer VLAN can result in unused IP addresses
- If the number of devices in the VLAN increases, the number of assigned address might not be large enough to accommodate them

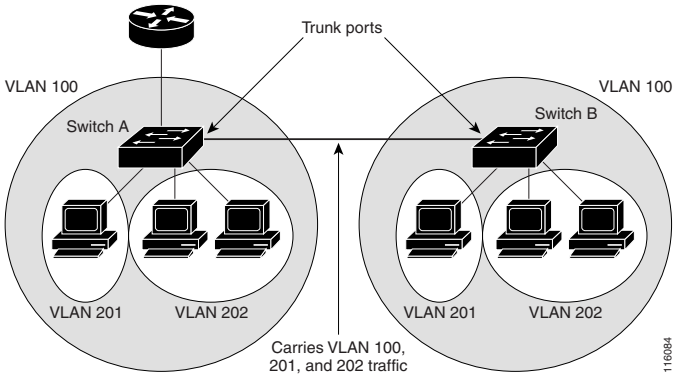
These problems are reduced by using private VLANs, where all members in the private VLAN share a common address space, which is allocated to the primary VLAN. Hosts are connected to secondary VLANs, and the DHCP server assigns them IP addresses from the block of addresses allocated to the

primary VLAN. Subsequent IP addresses can be assigned to customer devices in different secondary VLANs, but in the same primary VLAN. When new devices are added, the DHCP server assigns them the next available address from a large pool of subnet addresses.

Private VLANs across Multiple Switch Modules

As with regular VLANs, private VLANs can span multiple switch modules. A trunk port carries the primary VLAN and secondary VLANs to a neighboring switch module. The trunk port treats the private VLAN as any other VLAN. A feature of private VLANs across multiple switches is that traffic from an isolated port in Switch A does not reach an isolated port on Switch B. See Figure 12-2.

Figure 12-2 Private VLANs across Switch Modules



VLAN 100 = Primary VLAN
VLAN 201 = Secondary isolated VLAN
VLAN 202 = Secondary community VLAN

You must manually configure private VLANs on all switches in the Layer 2 network. If you do not configure the primary and secondary VLAN associations in some switches in the network, the Layer 2 databases in these switches are not merged. This can result in unnecessary flooding of private-VLAN traffic on those switches.

Private VLANs and Unicast, Broadcast and Multicast Traffic

In regular VLANs, devices in the same VLAN can communicate with each other at the Layer 2 level, but devices connected to interfaces in different VLANs must communicate at the Layer 3 level. In private VLANs, the promiscuous ports are members of the primary VLAN, while the host ports belong to secondary VLANs. Because the secondary VLAN is associated to the primary VLAN, members of the these VLANs can communicate with each other at the Layer 2 level.

In a regular VLAN, broadcasts are forwarded to all ports in that VLAN. Private-VLAN broadcast forwarding depends on the port sending the broadcast:

- An isolated port sends a broadcast only to the promiscuous ports or trunk ports.
- A community port sends a broadcast to all promiscuous ports, trunk ports, and ports in the same community VLAN.
- A promiscuous port (only NNI) sends a broadcast to all ports in the private VLAN (other promiscuous ports, trunk ports, isolated ports, and community ports).

Multicast traffic is routed or bridged across private-VLAN boundaries and within a single community VLAN. Multicast traffic is not forwarded between ports in the same isolated VLAN or between ports in different secondary VLANs.

Private VLANs and SVIs

In a Layer 3 switch module (a switch module running the IP services image), a switch module virtual interface (SVI) represents the Layer 3 interface of a VLAN. Layer 3 devices communicate with a private VLAN only through the primary VLAN and not through secondary VLANs. Configure Layer 3 VLAN interfaces only for primary VLANs. You cannot configure Layer 3 VLAN interfaces for secondary VLANs. SVIs for secondary VLANs are inactive while the VLAN is configured as a secondary VLAN.

- If you try to configure a VLAN with an active SVI as a secondary VLAN, the configuration is not allowed until you disable the SVI.
- If you try to create an SVI on a VLAN that is configured as a secondary VLAN and the secondary VLAN is already mapped at Layer 3, the SVI is not created, and an error is returned. If the SVI is not mapped at Layer 3, the SVI is created, but it is automatically shut down.

When the primary VLAN is associated with and mapped to the secondary VLAN, any configuration on the primary VLAN is propagated to the secondary VLAN SVIs. For example, if you assign an IP subnet to the primary VLAN SVI, this subnet is the IP subnet address of the entire private VLAN.

Configuring Private VLANs

Tasks for Configuring Private VLANs

To configure a private VLAN, follow these steps:

Step 1 Create the primary and secondary VLANs and associate them. See the "Configuring and Associating VLANs in a Private VLAN" section on page 12-9.

Note If the VLAN is not created already, the private-VLAN configuration process creates it.

Step 2 Configure interfaces to be isolated or community host ports, and assign VLAN membership to the host port. See the "Configuring a Layer 2 Interface as a Private-VLAN Host Port" section on page 12-11.

Step 3 Configure NNIs as promiscuous ports, and map the promiscuous ports to the primary-secondary VLAN pair. See the "Configuring a Layer 2 Interface as a Private-VLAN Promiscuous Port" section on page 12-12.

Step 4 If inter-VLAN routing will be used, configure the primary SVI, and map secondary VLANs to the primary. See the "Mapping Secondary VLANs to a Primary VLAN Layer 3 VLAN Interface" section on page 12-13.

Step 5 Verify private-VLAN configuration.

Default Private-VLAN Configuration

No private VLANs are configured. Newly created VLANs are UNI-ENI isolated VLANs.

Private-VLAN Configuration Guidelines

Guidelines for configuring private VLANs fall into these categories:

Secondary and Primary VLAN Configuration

Follow these guidelines when configuring private VLANs:

- You use VLAN configuration mode to configure private VLANs
- You must configure private VLANs on each device where you want private-VLAN ports
- A private VLAN cannot be a UNI-ENI VLAN.
  - To change a UNI-ENI isolated VLAN (the default) to a private VLAN, enter the **private-vlan** VLAN configuration command; this overwrites the default isolated VLAN configuration.
  - To change a UNI-ENI community VLAN to a private VLAN, you must first enter the **no uni-vlan** VLAN configuration command to return to the default UNI isolated VLAN configuration.
- You cannot configure VLAN 1 or VLANs 1002 to 1005 as primary or secondary VLANs. Extended VLANs (VLAN IDs 1006 to 4094) can belong to private VLANs
- A primary VLAN can have one isolated VLAN and multiple community VLANs associated with it. An isolated or community VLAN can have only one primary VLAN associated with it.
- Although a private VLAN contains more than one VLAN, only one Spanning Tree Protocol (STP) instance runs for the entire private VLAN. When a secondary VLAN is associated with the primary VLAN, the STP parameters of the primary VLAN are propagated to the secondary VLAN.
- You can enable DHCP snooping on private VLANs. When you enable DHCP snooping on the primary VLAN, it is propagated to the secondary VLANs. If you configure DHCP on a secondary VLAN, the configuration does not take effect if the primary VLAN is already configured.
- If you enable IP source guard on private-VLAN ports, you must enable DHCP snooping on the primary VLAN.

- You can apply different quality of service (QoS) configurations to primary, isolated, and community VLANs.
- When the switch module is running the IP services image, for sticky ARP
  - Sticky ARP entries are those learned on SVIs and Layer 3 interfaces. The entries do not age out.
  - The **ip sticky-arp** global configuration command is supported only on SVIs belonging to private VLANs.
  - The **ip sticky-arp** interface configuration command is only supported on

    Layer 3 interfaces

    SVIs belonging to normal VLANs

    SVIs belonging to private VLANs

  For more information about using the **ip sticky-arp** *global* configuration and the **ip sticky-arp** *interface* configuration commands, see the command reference for this release.
- You can configure VLAN maps on primary and secondary VLANs. However, we recommend that you configure the same VLAN maps on private-VLAN primary and secondary VLANs.
- When a frame is forwarded through Layer 2 within a private VLAN, the same VLAN map is applied at the receiving and sending sides. When a frame is routed from inside a private VLAN to an external port, the private-VLAN map is applied at the receiving side.
  - For frames going upstream from a host port to a promiscuous port, the VLAN map configured on the secondary VLAN is applied.
  - For frames going downstream from a promiscuous port to a host port, the VLAN map configured on the primary VLAN is applied.

  To filter out specific IP traffic for a private VLAN, you should apply the VLAN map to both the primary and secondary VLANs.
- If the switch module is running the IP services image, you can apply router ACLs only on the primary-VLAN SVIs. The ACL is applied to both primary and secondary VLAN Layer 3 traffic.
- Although private VLANs provide host isolation at Layer 2, hosts can communicate with each other at Layer 3.
- Private VLANs support these Switched Port Analyzer (SPAN) features:
  - You can configure a private-VLAN port as a SPAN source port.
  - You can use VLAN-based SPAN (VSPAN) on primary, isolated, and community VLANs or use SPAN on only one VLAN to separately monitor sent or received traffic.

Private-VLAN Port Configuration

Follow these guidelines when configuring private-VLAN ports:

- Promiscuous ports must be NNIs; UNIs and ENIs cannot be configured as promiscuous ports.
- Use only the private-VLAN configuration commands to assign ports to primary, isolated, or community VLANs. Layer 2 access ports assigned to the VLANs that you configure as primary, isolated, or community VLANs are inactive while the VLAN is part of the private-VLAN configuration. Layer 2 trunk interfaces remain in the STP forwarding state.
- Do not configure NNI ports that belong to a Link Aggregation Control Protocol (LACP) EtherChannel as private-VLAN ports. While a port is part of the private-VLAN configuration, any EtherChannel configuration for it is inactive.

- Enable Port Fast and BPDU guard on NNI isolated and community host ports to prevent STP loops due to misconfigurations and to speed up STP convergence. When enabled, STP applies the BPDU guard feature to all Port Fast-configured Layer 2 LAN ports. Do not enable Port Fast and BPDU guard on promiscuous ports.
- If you delete a VLAN used in the private-VLAN configuration, the private-VLAN ports associated with the VLAN become inactive.
- Private-VLAN ports can be on different network devices if the devices are trunk-connected and the primary and secondary VLANs have not been removed from the trunk.
- A community private VLAN can include no more than eight UNIs and ENIs. If you try to add more than eight, the configuration is not allowed. If you try to configure a VLAN that includes a combination of more than eight UNIs and ENIs as a community private VLAN, the configuration is not allowed.

Limitations with Other Features

When configuring private VLANs, remember these limitations with other features:

Note In some cases, the configuration is accepted with no error messages, but the commands have no effect.

- When IGMP snooping is enabled on the switch module (the default), the switch module supports no more than 20 private-VLAN domains.
- A private VLAN cannot be a UNI-ENI isolated or UNI-ENI community VLAN. For more information about UNI-ENI VLANs, see Chapter 11, “VLAN Configuration.”
- Do not configure a remote SPAN (RSPAN) VLAN as a private-VLAN primary or secondary VLAN.
- Do not configure private-VLAN ports on interfaces configured for these other features:
  - dynamic-access port VLAN membership
  - LACP (only NNIs or ENIs)
- Multicast VLAN Registration (MVR)
- You can configure 802.1x port-based authentication on a private-VLAN port, but do not configure IEEE 802.1x with port security on private-VLAN ports.
- A private-VLAN host or promiscuous port cannot be a SPAN destination port. If you configure a SPAN destination port as a private-VLAN port, the port becomes inactive.
- If you configure a static MAC address on a promiscuous port in the primary VLAN, you must add the same static address to all associated secondary VLANs. If you configure a static MAC address on a host port in a secondary VLAN, you must add the same static MAC address to the associated primary VLAN. When you delete a static MAC address from a private-VLAN port, you must remove all instances of the configured MAC address from the private VLAN.

  Note Dynamic MAC addresses learned in one VLAN of a private VLAN are replicated in the associated VLANs. For example, a MAC address learned in a secondary VLAN is replicated in the primary VLAN. When the original dynamic MAC address is deleted or aged out, the replicated addresses are removed from the MAC address table.

- Configure Layer 3 VLAN interfaces only for primary VLANs.

Configuring and Associating VLANs in a Private VLAN

Beginning in privileged EXEC mode, follow these steps to configure a private VLAN:

Note The **private-vlan** commands do not take effect until you exit VLAN configuration mode.

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter VLAN configuration mode and designate or create a VLAN that will be the primary VLAN. The VLAN ID range is 2 to 1001 and 1006 to 4094. **Note** If the VLAN has been configured as a UNI-ENI community VLAN, you must enter the **no uni-vlan** VLAN configuration command before configuring a private VLAN.	**vlan** *vlan-id*
Step 3	Designate the VLAN as the primary VLAN.	**private-vlan primary**
Step 4	Return to global configuration mode.	**exit**
Step 5	(Optional) Enter VLAN configuration mode and designate or create a VLAN that will be an isolated VLAN. The VLAN ID range is 2 to 1001 and 1006 to 4094.	**vlan** *vlan-id*
Step 6	Designate the VLAN as an isolated VLAN.	**private-vlan isolated**
Step 7	Return to global configuration mode.	**exit**
Step 8	(Optional) Enter VLAN configuration mode and designate or create a VLAN that will be a community VLAN. The VLAN ID range is 2 to 1001 and 1006 to 4094. **Note** If the VLAN has been configured as a UNI-ENI community VLAN, you must enter the **no uni-vlan** VLAN configuration command before configuring a private VLAN.	**vlan** *vlan-id*
Step 9	Designate the VLAN as a community VLAN.	**private-vlan community**
Step 10	Return to global configuration mode.	**exit**
Step 11	Enter VLAN configuration mode for the primary VLAN designated in Step 3.	**vlan** *vlan-id*
Step 12	Associate the secondary VLANs with the primary VLAN.	**private-vlan association** [**add** | **remove**] *secondary_vlan_list*
Step 13	Return to privileged EXEC mode.	**end**

	Step	Command
Step 14	Verify the configuration.	**show vlan private-vlan** [**type**] or **show interfaces status**
Step 15	(Optional) Save your entries in the switch module startup configuration file.	**copy running-config startup config**

When you associate secondary VLANs with a primary VLAN, note this syntax information:

- The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs.
- The *secondary_vlan_list* parameter can contain multiple community VLAN IDs but only one isolated VLAN ID.
- Enter a *secondary_vlan_list,* or use the **add** keyword with a *secondary_vlan_list* to associate secondary VLANs with a primary VLAN.
- Use the **remove** keyword with a *secondary_vlan_list* to clear the association between secondary VLANs and a primary VLAN.
- The **private-vlan association** VLAN configuration command does not take effect until you exit VLAN configuration mode.

This example shows how to configure VLAN 20 as a primary VLAN, VLAN 501 as an isolated VLAN, and VLANs 502 and 503 as community VLANs, to associate them in a private VLAN, and to verify the configuration. It assumes that VLANs 502 and 503 have previously been configured as UNI-ENI community VLANs:

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 501
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 502
Switch(config-vlan)# no-uni vlan
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 503
Switch(config-vlan)# no-uni vlan
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan association 501-503
Switch(config-vlan)# end
Switch(config)# show vlan private vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
20      501       isolated
20      502       community
20      503       community
20      504       non-operational
```

Configuring a Layer 2 Interface as a Private-VLAN Host Port

Beginning in privileged EXEC mode, follow these steps to configure a Layer 2 interface as a private-VLAN host port and to associate it with primary and secondary VLANs:

Note Isolated and community VLANs are both secondary VLANs.

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode for the Layer 2 interface to be configured.	**interface** *interface-id*
Step 3	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.	**no shutdown**
Step 4	Configure the Layer 2 port as a private-VLAN host port.	**switchport mode private-vlan host**
Step 5	Associate the Layer 2 port with a private VLAN.	**switchport private-vlan host-association** *primary_vlan_id secondary_vlan_id*
Step 6	Return to privileged EXEC mode.	**end**
Step 7	Verify the configuration.	**show interfaces** [*interface-id*] **switchport**
Step 8	(Optional) Save your entries in the switch module startup configuration file.	**copy running-config startup config**

This example shows how to configure an interface as a private-VLAN host port, associate it with a private-VLAN pair, and verify the configuration:

```
Switch# configure terminal
Switch(config)# interface fastethernet0/9
Switch(config-if)# no shutdown
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 501
Switch(config-if)# end
Switch# show interfaces fastethernet0/9 switchport
Name: Fa0/9
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Administrative private-vlan host-association: 20 501
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan:
```

```
20 501
<output truncated>
```

Configuring a Layer 2 Interface as a Private-VLAN Promiscuous Port

You can configure only NNIs as promiscuous ports. Beginning in privileged EXEC mode, follow these steps to configure a Layer 2 interface as a private-VLAN promiscuous port and map it to primary and secondary VLANs:

Note Isolated and community VLANs are both secondary VLANs.

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode for the Layer 2 interface to be configured. The interface must be an NNI. **Note** If the interface is a UNI or ENI, you must enter the **port-type nni** interface configuration command before configuring it as a promiscuous port.	**interface** *interface-id*
Step 3	Configure the Layer 2 NNI port as a private-VLAN promiscuous port.	**switchport mode private-vlan promiscuous**
Step 4	Map the private-VLAN promiscuous port to a primary VLAN and to selected secondary VLANs.	**switchport private-vlan mapping** *primary_vlan_id* {**add** | **remove**} *secondary_vlan_list*
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify the configuration.	**show interfaces** [*interface-id*] **switchport**
Step 7	(Optional) Save your entries in the switch module startup configuration file.	**copy running-config startup config**

When you configure a Layer 2 interface as a private-VLAN promiscuous port, note this syntax information:

- The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs.
- Enter a *secondary_vlan_list*, or use the **add** keyword with a *secondary_vlan_list* to map the secondary VLANs to the private-VLAN promiscuous port.
- Use the **remove** keyword with a *secondary_vlan_list* to clear the mapping between secondary VLANs and the private-VLAN promiscuous port.

This example shows how to configure an NNI as a private-VLAN promiscuous port and map it to a private VLAN. The interface is a member of primary VLAN 20 and secondary VLANs 501 to 503 are mapped to it.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/0/0
```

```
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 add 501-503
Switch(config-if)# end
```

Use the **show vlan private-vlan** or the **show interface status** privileged EXEC command to display primary and secondary VLANs and private-VLAN ports on the switch module.

Note Private VLAN configuration is not recommended on FastEthernet ports FE0/9 to FE0/16 on the GRWIC-D-ES-2S-8PC (Copper model) and the FastEthernet ports FE0/5 to FE0/12 on the GRWIC-D-ES-6S (SFP model). For Private VLAN configuration on the backplane, we recommend using PortChannel48. For details, see Chapter 9, "EtherChannel Configuration Between the Switch Module and the Host Router."

Mapping Secondary VLANs to a Primary VLAN Layer 3 VLAN Interface

If the switch module is running the IP services image and the private VLAN will be used for inter-VLAN routing, you configure an SVI for the primary VLAN and map secondary VLANs to the SVI.

Note Isolated and community VLANs are both secondary VLANs.

Beginning in privileged EXEC mode, follow these steps to map secondary VLANs to the SVI of a primary VLAN to allow Layer 3 switching of private-VLAN traffic:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode for the primary VLAN, and configure the VLAN as an SVI. The VLAN ID range is 2 to 1001 and 1006 to 4094.	**interface vlan** *primary_vlan_id*
Step 3	Map the secondary VLANs to the Layer 3 VLAN interface of a primary VLAN to allow Layer 3 switching of private-VLAN incoming traffic.	**private-vlan mapping** [**add** | **remove**] *secondary_vlan_list*
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify the configuration.	**show interface private-vlan mapping**
Step 6	(Optional) Save your entries in the switch module startup configuration file.	**copy running-config startup config**

Note The **private-vlan mapping** interface configuration command only affects private-VLAN traffic that is switched through Layer 3.

When you map secondary VLANs to the Layer 3 VLAN interface of a primary VLAN, note this syntax information:

- The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs.

- Enter a *secondary_vlan_list,* or use the **add** keyword with a *secondary_vlan_list* to map the secondary VLANs to the primary VLAN.
- Use the **remove** keyword with a *secondary_vlan_list* to clear the mapping between secondary VLANs and the primary VLAN.

This example shows how to map the interfaces of VLANs 501 and 502 to primary VLAN 10, which permits routing of secondary VLAN incoming traffic from private VLANs 501 to 502:

```
Switch# configure terminal
Switch(config)# interface vlan 10
Switch(config-if)# private-vlan mapping 501-502
Switch(config-if)# end
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan10    501            isolated
vlan10    502            community
```

Monitoring Private VLANs

Table 12-1 shows the privileged EXEC commands for monitoring private-VLAN activity.

Table 12-1 Private VLAN Monitoring Commands

Command	Description
show interfaces status	Displays the status of interfaces, including the VLANs to which they belong.
show vlan private-vlan [**type**]	Display the private-VLAN information for the switch module.
show interface switchport	Display the private-VLAN configuration on interfaces.
show interface private-vlan mapping	Display information about the private-VLAN mapping for VLAN interfaces.

This is an example of the output from the **show vlan private-vlan** command:

```
Switch(config)# show vlan private-vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
10      501       isolated          Fa0/1, Gi0/1, Gi0/2
10      502       community         Fa0/11, Fa0/12, Gi0/1
10      503       non-operational
```

IEEE 802.1Q and Layer 2 Protocol Tunneling Configuration

Virtual private networks (VPNs) provide enterprise-scale connectivity on a shared infrastructure, often Ethernet-based, with the same security, prioritization, reliability, and manageability requirements of private networks.

Tunneling is a feature designed for service providers who carry traffic of multiple customers across their networks and are required to maintain the VLAN and Layer 2 protocol configurations of each customer without impacting the traffic of other customers. The CGR 2010 ESM supports IEEE 802.1Q tunneling and Layer 2 protocol tunneling when it is running the IP services image.

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

This chapter contains the following topics:

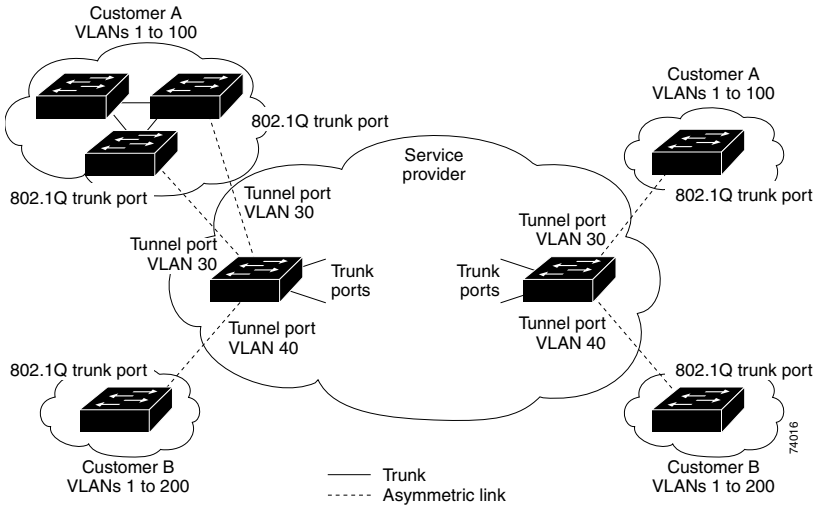
Understanding IEEE 802.1Q Tunneling

Business customers of service providers often have specific requirements for VLAN IDs and the number of VLANs to be supported. The VLAN ranges required by different customers in the same service-provider network might overlap, and traffic of customers through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations and could easily exceed the VLAN limit (4096) of the IEEE 802.1Q specification.

Using the IEEE 802.1Q tunneling feature, service providers can use a single VLAN to support customers who have multiple VLANs. Customer VLAN IDs are preserved, and traffic from different customers is segregated within the service-provider network, even when they appear to be in the same VLAN. Using IEEE 802.1Q tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy and retagging the tagged packets. A port configured to support IEEE 802.1Q tunneling is called a *tunnel port*. When you configure tunneling, you assign a tunnel port to a VLAN ID that is dedicated to tunneling. Each customer requires a separate service-provider VLAN ID, but that VLAN ID supports all of the customer's VLANs.

Customer traffic tagged in the normal way with appropriate VLAN IDs comes from an IEEE 802.1Q trunk port on the customer device and into a tunnel port on the service-provider edge switch module. The link between the customer device and the edge switch module is asymmetric because one end is configured as an IEEE 802.1Q trunk port, and the other end is configured as a tunnel port. You assign the tunnel port interface to an access VLAN ID that is unique to each customer. See Figure 13-1.

Figure 13-1 IEEE 802.1Q Tunnel Ports in a Service-Provider Network

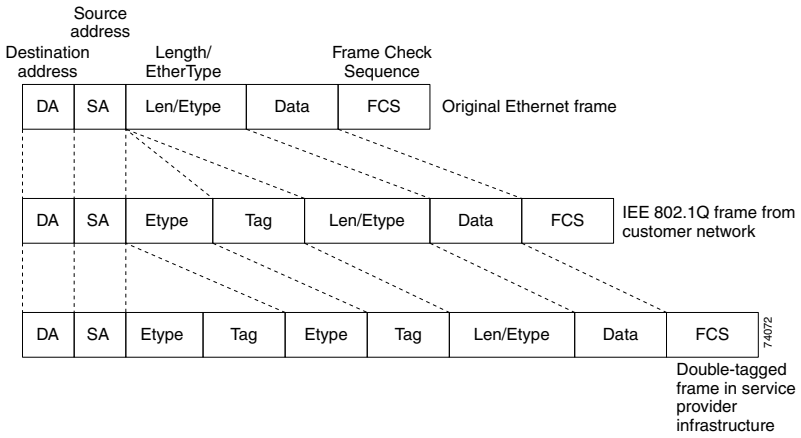


Packets coming from the customer trunk port into the tunnel port on the service-provider edge switch module are normally IEEE 802.1Q-tagged with the appropriate VLAN ID. The the tagged packets remain intact inside the switch module and when they exit the trunk port into the service-provider network, they are encapsulated with another layer of an IEEE 802.1Q tag (called the *metro tag*) that contains the VLAN ID that is unique to the customer. The original customer IEEE 802.1Q tag is preserved in the encapsulated packet. Packets entering the service-provider network are double-tagged, with the outer (metro) tag containing the customer's access VLAN ID, and the inner VLAN ID being that of the incoming traffic.

When the double-tagged packet enters another trunk port in a service-provider core switch module, the outer tag is stripped as the switch module processes the packet. When the packet exits another trunk port on the same core switch module, the same metro tag is again added to the packet. Figure 13-2 shows the tag structures of the double-tagged packets.

Note Remove the Layer 2 protocol configuration from a trunk port because incoming encapsulated packets change that trunk port to error disabled. The outgoing encapsulated VTP (CDP and STP) packets are dropped on that trunk.

Figure 13-2 Original (Normal), IEEE 802.1Q, and Double-Tagged Ethernet Packet Formats



When the packet enters the trunk port of the service-provider egress switch module, the outer tag is again stripped as the switch module internally processes the packet. The metro tag is not added when the packet is sent out the tunnel port on the edge switch module into the customer network. The packet is sent as a normal IEEE 802.1Q-tagged frame to preserve the original VLAN numbers in the customer network.

In Figure 13-1, Customer A was assigned VLAN 30, and Customer B was assigned VLAN 40. Packets entering the edge switch module tunnel ports with IEEE 802.1Q tags are double-tagged when they enter the service-provider network, with the outer tag containing VLAN ID 30 or 40, appropriately, and the inner tag containing the original VLAN number, for example, VLAN 100. Even if both Customers A and B have VLAN 100 in their networks, the traffic remains segregated within the service-provider network because the outer tag is different. Each customer controls its own VLAN numbering space, which is independent of the VLAN numbering space used by other customers and the VLAN numbering space used by the service-provider network.

At the outbound tunnel port, the original VLAN numbers on the customer's network are recovered. It is possible to have multiple levels of tunneling and tagging, but the switch module supports only one level in this release.

If traffic coming from a customer network is not tagged (native VLAN frames), these packets are bridged or routed as normal packets. All packets entering the service-provider network through a tunnel port on an edge switch module are treated as untagged packets, whether they are untagged or already tagged with IEEE 802.1Q headers. The packets are encapsulated with the metro tag VLAN ID (set to the access VLAN of the tunnel port) when they are sent through the service-provider network on an IEEE 802.1Q trunk port. The priority field on the metro tag is set to the interface class of service (CoS) priority configured on the tunnel port. (The default is zero if none is configured.)

Configuring IEEE 802.1Q Tunneling

These sections contain this configuration information:

Default IEEE 802.1Q Tunneling Configuration

By default, IEEE 802.1Q tunneling is disabled because the default switch moduleport mode is dynamic auto. Tagging of IEEE 802.1Q native VLAN packets on all IEEE 802.1Q trunk ports is also disabled.

IEEE 802.1Q Tunneling Configuration Guidelines

When you configure IEEE 802.1Q tunneling, you should always use an asymmetrical link between the customer device and the edge switch module, with the customer device port configured as an IEEE 802.1Q trunk port and the edge switch module port configured as a tunnel port.

Assign tunnel ports only to VLANs that are used for tunneling.

Configuration requirements for native VLANs and for and maximum transmission units (MTUs) are explained in these next sections.

Native VLANs

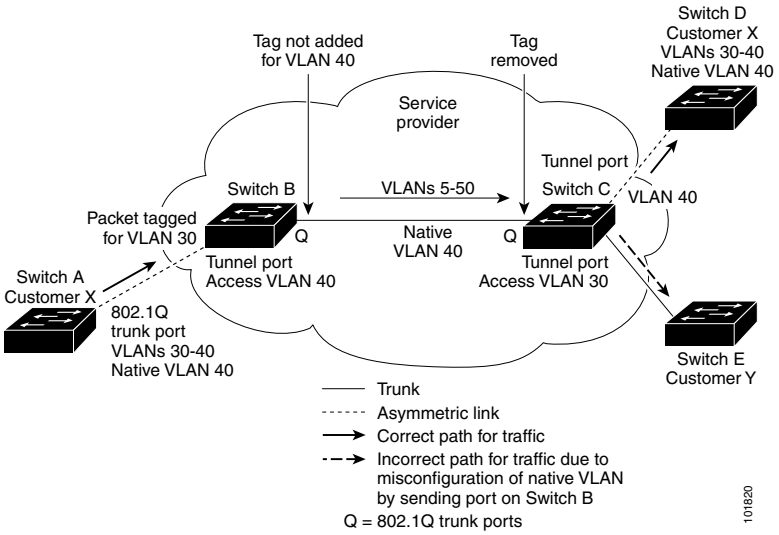
When configuring IEEE 802.1Q tunneling on an edge switch module, you must use IEEE 802.1Q trunk ports for sending packets into the service-provider network. However, packets going through the core of the service-provider network can be carried through IEEE 802.1Q trunks, ISL trunks, or nontrunking links. When IEEE 802.1Q trunks are used in these core switches, the native VLANs of the IEEE 802.1Q trunks must not match any native VLAN of the nontrunking (tunneling) port on the same switch module because traffic on the native VLAN would not be tagged on the IEEE 802.1Q sending trunk port.

See Figure 13-3. VLAN 40 is configured as the native VLAN for the IEEE 802.1Q trunk port from Customer X at the ingress edge switch module in the service-provider network (Switch B). Switch A of Customer X sends a tagged packet on VLAN 30 to the ingress tunnel port of Switch B in the service-provider network, which belongs to access VLAN 40. Because the access VLAN of the tunnel port (VLAN 40) is the same as the native VLAN of the edge-switch module trunk port (VLAN 40), the metro tag is not added to tagged packets received from the tunnel port. The packet carries only the VLAN 30 tag through the service-provider network to the trunk port of the egress-edge switch module (Switch C) and is misdirected through the egress switch module tunnel port to Customer Y.

These are some ways to solve this problem:

- Use the **vlan dot1q tag native** global configuration command to configure the edge switch module so that all packets going out an IEEE 802.1Q trunk, including the native VLAN, are tagged. If the switch module is configured to tag native VLAN packets on all IEEE 802.1Q trunks, the switch module accepts untagged packets, but sends only tagged packets.
- Ensure that the native VLAN ID on the edge-switch module trunk port is not within the customer VLAN range. For example, if the trunk port carries traffic of VLANs 100 to 200, assign the native VLAN a number outside that range.

Figure 13-3 Potential Problem with IEEE 802.1Q Tunneling and Native VLANs



System MTU

The default system MTU for traffic on the switch module is 1500 bytes. You can configure Fast Ethernet ports to support frames larger than 1500 bytes by using the **system mtu** global configuration command. You can configure Gigabit Ethernet ports to support frames larger than 1500 bytes by using the **system mtu jumbo** global configuration command. Because the IEEE 802.1Q tunneling feature increases the frame size by 4 bytes when the metro tag is added, you must configure all switches in the service-provider network to be able to process maximum frames by increasing the switch module system MTU size to at least 1504 bytes. The maximum allowable system MTU for Gigabit Ethernet interfaces is 9000 bytes; the maximum system MTU for Fast Ethernet interfaces is 1998 bytes.

IEEE 802.1Q Tunneling and Other Features

Although IEEE 802.1Q tunneling works well for Layer 2 packet switching, there are incompatibilities between some Layer 2 features and Layer 3 switching.

- A tunnel port cannot be a routed port.
- IP routing is not supported on a VLAN that includes IEEE 802.1Q ports. Packets received from a tunnel port are forwarded based only on Layer 2 information. If routing is enabled on a switch module virtual interface (SVI) that includes tunnel ports, untagged IP packets received from the tunnel port are recognized and routed by the switch module. Customer can access the internet through its native VLAN. If this access is not needed, you should not configure SVIs on VLANs that include tunnel ports.
- Fallback bridging is not supported on tunnel ports. Because all IEEE 802.1Q-tagged packets received from a tunnel port are treated as non-IP packets, if fallback bridging is enabled on VLANs that have tunnel ports configured, IP packets would be improperly bridged across VLANs. You must *not* enable fallback bridging on VLANs with tunnel ports.
- Tunnel ports do not support IP access control lists (ACLs).
- Layer 3 quality of service (QoS) ACLs and other QoS features related to Layer 3 information are not supported on tunnel ports. MAC-based QoS is supported on tunnel ports.

- EtherChannel port groups are compatible with tunnel ports as long as the IEEE 802.1Q configuration is consistent within an EtherChannel port group.
- Link Aggregation Control Protocol (LACP) and UniDirectional Link Detection (UDLD) are supported on IEEE 802.1Q tunnel ports.
- Dynamic Trunking Protocol (DTP) is not compatible with IEEE 802.1Q tunneling because you must manually configure asymmetric links with tunnel ports and trunk ports.
- VLAN Trunking Protocol (VTP) does not work between devices that are connected by an asymmetrical link or devices that communicate through a tunnel.
- Loopback detection is supported on IEEE 802.1Q tunnel ports.
- When a port is configured as an IEEE 802.1Q tunnel port, spanning-tree bridge protocol data unit (BPDU) filtering is automatically enabled on the interface. Cisco Discovery Protocol (CDP) and the Layer Link Discovery Protocol (LLDP) are automatically disabled on the interface.

Configuring an IEEE 802.1Q Tunneling Port

Beginning in privileged EXEC mode, follow these steps to configure a port as an IEEE 802.1Q tunnel port:

	Steps	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode for the interface to be configured as a tunnel port. This should be the edge port in the service-provider network that connects to the customer switch module. Valid interfaces include physical interfaces and port-channel logical interfaces (port channels 1 to 48).	**interface** *interface-id*
Step 3	Specify the default VLAN, which is used if the interface stops trunking. This VLAN ID is specific to the particular customer.	**switchport access vlan** *vlan-id*
Step 4	Set the interface as an IEEE 802.1Q tunnel port.	**switchport mode dot1q-tunnel**
Step 5	Return to global configuration mode.	**exit**
Step 6	(Optional) Set the switch module to enable tagging of native VLAN packets on all IEEE 802.1Q trunk ports. When not set, and a customer VLAN ID is the same as the native VLAN, the trunk port does not apply a metro tag, and packets could be sent to the wrong destination.	**vlan dot1q tag native**
Step 7	Return to privileged EXEC mode.	**end**
Step 8	Display the ports configured for IEEE 802.1Q tunneling. Display the ports that are in tunnel mode.	**show running-config** **show dot1q-tunnel**

	Steps	Command
Step 9	Display IEEE 802.1Q native VLAN tagging status.	**show vlan dot1q tag native**
Step 10	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

Use the **no switchport mode dot1q-tunnel** interface configuration command to return the port to the default state of dynamic desirable. Use the **no vlan dot1q tag native** global configuration command to disable tagging of native VLAN packets.

This example shows how to configure an interface as a tunnel port, enable tagging of native VLAN packets, and verify the configuration. In this configuration, the VLAN ID for the customer connected to Gigabit Ethernet interface 7 is VLAN 22:

```
Switch(config)# interface gigabitethernet0/0/0
Switch(config-if)# switchport access vlan 22
% Access VLAN does not exist. Creating vlan 22
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# exit
Switch(config)# vlan dot1q tag native
Switch(config)# end
Switch# show dot1q-tunnel interface gigabitethernet0/0/0
Port
-----
Gi10/0/0Port

-----
Switch# show vlan dot1q tag native
dot1q native vlan tagging is enabled
```

Understanding Layer 2 Protocol Tunneling

Customers at different sites connected across a service-provider network need to use various Layer 2 protocols to scale their topologies to include all remote sites, as well as the local sites. STP must run properly, and every VLAN should build a proper spanning tree that includes the local site and all remote sites across the service-provider network. Cisco Discovery Protocol (CDP) must discover neighboring Cisco devices from local and remote sites. VLAN Trunking Protocol (VTP) must provide consistent VLAN configuration throughout all sites in the customer network.

When protocol tunneling is enabled, edge switches on the inbound side of the service-provider network encapsulate Layer 2 protocol packets with a special MAC address and send them across the service-provider network. Core switches in the network do not process these packets but forward them as normal packets. Layer 2 protocol data units (PDUs) for CDP, STP, or VTP cross the service-provider network and are delivered to customer switches on the outbound side of the service-provider network. Identical packets are received by all customer ports on the same VLANs with these results:

- Users on each of a customer's sites can properly run STP, and every VLAN can build a correct spanning tree based on parameters from all sites and not just from the local site
- CDP discovers and shows information about the other Cisco devices connected through the service-provider network

- VTP provides consistent VLAN configuration throughout the customer network, propagating to all switches through the service provider

Note To provide interoperability with third-party vendors, you can use the Layer 2 protocol-tunnel bypass feature. Bypass mode transparently forwards control PDUs to vendor switches that have different ways of controlling protocol tunneling. You implement bypass mode by enabling Layer 2 protocol tunneling on the egress trunk port. When Layer 2 protocol tunneling is enabled on the trunk port, the encapsulated tunnel MAC address is removed and the protocol packets have their normal MAC address.

Layer 2 protocol tunneling can be used independently or can enhance IEEE 802.1Q tunneling. If protocol tunneling is not enabled on IEEE 802.1Q tunneling ports, remote switches at the receiving end of the service-provider network do not receive the PDUs and cannot properly run STP, CDP, and VTP. When protocol tunneling *is* enabled, Layer 2 protocols within each customer's network are totally separate from those running within the service-provider network. Customer switches on different sites that send traffic through the service-provider network with IEEE 802.1Q tunneling achieve complete knowledge of the customer's VLAN. If IEEE 802.1Q tunneling is not used, you can still enable Layer 2 protocol tunneling by connecting to the customer switch module through access ports and by enabling tunneling on the service-provider access port.

For example, in Figure 13-4, Customer X has four switches in the same VLAN, that are connected through the service-provider network. If the network does not tunnel PDUs, switches on the far ends of the network cannot properly run STP, CDP, and VTP. For example, STP for a VLAN on a switch module in Customer X, Site 1, will build a spanning tree on the switches at that site without considering convergence parameters based on Customer X's switch module in Site 2. This could result in the topology shown in Figure 13-5.

Figure 13-4 Layer 2 Protocol Tunneling

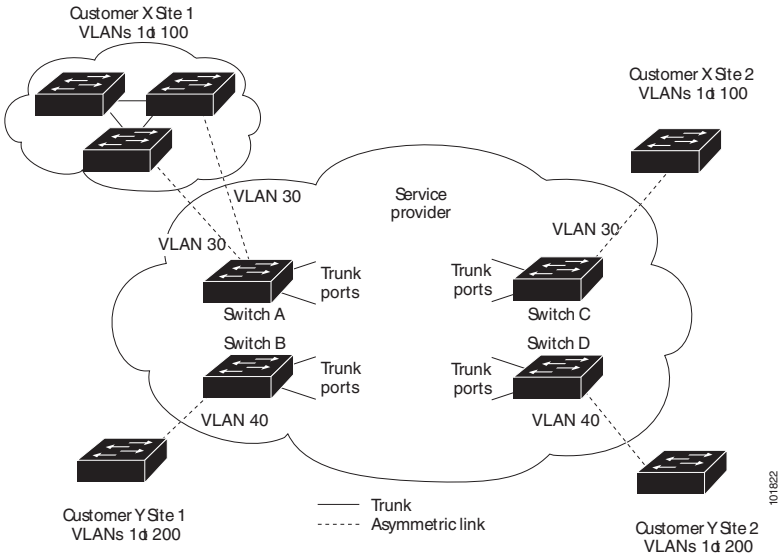
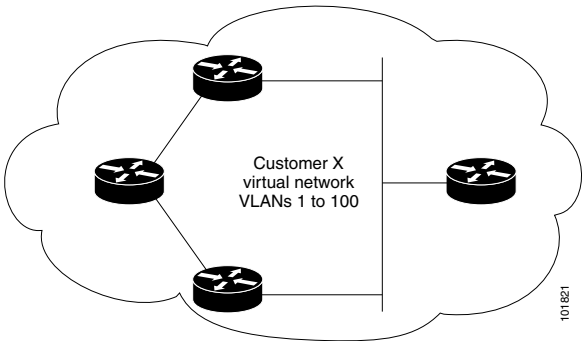


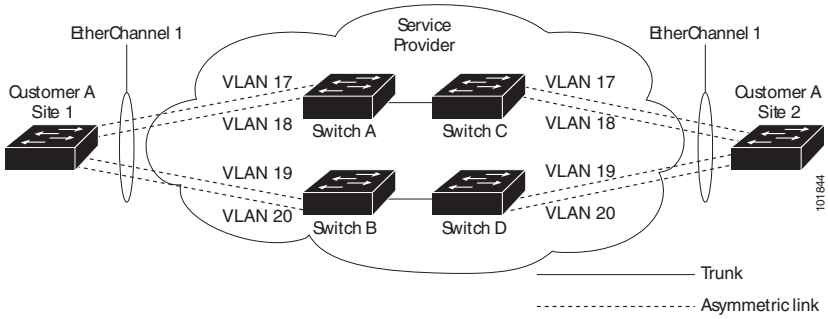
Figure 13-5 Layer 2 Network Topology without Proper Convergence



In aservice-provider network, you can use Layer 2 protocol tunneling to enhance the creation of EtherChannels by emulating a point-to-point network topology. When you enable protocol tunneling (LACP) on the SP switch module, remote customer switches receive the PDUs and can negotiate the automatic creation of EtherChannels.

For example, in Figure 13-6, Customer A has two switches in the same VLAN that are connected through theservice-provider network. When the network tunnels PDUs, switches on the far ends of the network can negotiate the automatic creation of EtherChannels without needing dedicated lines. See the "Configuring Layer 2 Tunneling for EtherChannels" section on page 13-14 for instructions.

Figure 13-6 Layer 2 Protocol Tunneling for EtherChannels



Configuring Layer 2 Protocol Tunneling

You can enable Layer 2 protocol tunneling (by protocol) on the ports that are connected to the customer in the edge switches of the service-provider network. The service-provider edge switches connected to the customer switch module perform the tunneling process. Edge-switch module tunnel ports are connected to customer IEEE 802.1Q trunk ports. Edge-switch module access ports are connected to customer access ports. The edge switches connected to the customer switch module perform the tunneling process.

You can enable Layer 2 protocol tunneling on ports that are configured as access ports or tunnel ports. You cannot enable Layer 2 protocol tunneling on ports configured in either **switchport mode dynamic auto (the default mode)** or **switchport mode dynamic desirable**.

The switch module supports Layer 2 protocol tunneling for CDP, STP, and VTP. For emulated point-to-point network topologies, it also supports LACP and UDLD protocols. The switch module does not support Layer 2 protocol tunneling for LLDP.

Caution LACP and UDLD protocol tunneling is only intended to emulate a point-to-point topology. An erroneous configuration that sends tunneled packets to many ports could lead to a network failure.

When the Layer 2 PDUs that entered the service-provider inbound edge switch module through a Layer 2 protocol-enabled port exit through the trunk port into the service-provider network, the switch module overwrites the customer PDU-destination MAC address with a well-known Cisco proprietary multicast address (01-00-0c-cd-cd-d0). If IEEE 802.1Q tunneling is enabled, packets are also double-tagged; the outer tag is the customer metro tag, and the inner tag is the customer's VLAN tag. The core switches ignore the inner tags and forward the packet to all trunk ports in the same metro VLAN. The edge switches on the outbound side restore the proper Layer 2 protocol and MAC address information and forward the packets to all tunnel or access ports in the same metro VLAN. The Layer 2 PDUs remain intact and are delivered across the service-provider infrastructure to the other side of the customer network.

See Figure 13-4 on page 13-8, with Customer X and Customer Y in access VLANs 30 and 40, respectively. Asymmetric links connect the customers in Site 1 to edge switches in the service-provider network. The Layer 2 PDUs (for example, BPDUs) coming into Switch 2 from Customer Y in Site 1 are forwarded to the infrastructure as double-tagged packets with the well-known MAC address as the destination MAC address. These double-tagged packets have the metro VLAN tag of 40, as well as an inner VLAN tag (for example, VLAN 100). When the double-tagged packets enter Switch D, the outer VLAN tag 40 is removed, the well-known MAC address is replaced with the respective Layer 2 protocol MAC address, and the packet is sent to Customer Y on Site 2 as a single-tagged frame in VLAN 100.

You can also enable Layer 2 protocol tunneling on access ports on the edge switch module connected to access or trunk ports on the customer switch module. In this case, the encapsulation and decapsulation process is the same as described in the previous paragraph, except that the packets are not double-tagged in the service-provider network. The single tag is the customer-specific access VLAN tag.

These sections contain this configuration information:

Default Layer 2 Protocol Tunneling Configuration

Table 13-1 shows the default Layer 2 protocol tunneling configuration.

Table 13-1 Default Layer 2 Ethernet Interface VLAN Configuration

Feature	Default Setting
Layer 2 protocol tunneling	Disabled
Shutdown threshold	None set

Table 13-1 Default Layer 2 Ethernet Interface VLAN Configuration (continued)

Feature	Default Setting
Drop threshold	None set
CoS value	If a CoS value is configured on the interface, that value is used to set the BPDU CoS value for Layer 2 protocol tunneling. If no CoS value is configured at the interface level, the default value for CoS marking of L2 protocol tunneling BPDUs is 5. This does not apply to data traffic.

Layer 2 Protocol Tunneling Configuration Guidelines

These are some configuration guidelines and operating characteristics of Layer 2 protocol tunneling:

- The switch module supports tunneling of CDP, STP, including multiple STP (MSTP), and VTP. Protocol tunneling is disabled by default but can be enabled for the individual protocols on IEEE 802.1Q tunnel ports or access ports.
- The switch module does not support Layer 2 protocol tunneling on ports with **switchport mode dynamic auto** or **dynamic desirable**.
- DTP is not compatible with layer 2 protocol tunneling.
- The edge switches on the outbound side of the service-provider network restore the proper Layer 2 protocol and MAC address information and forward the packets to all tunnel and access ports in the same metro VLAN.
- For interoperability with third-party vendor switches, the switch module supports a Layer 2 protocol-tunnel bypass feature. Bypass mode transparently forwards control PDUs to vendor switches that have different ways of controlling protocol tunneling.When Layer 2 protocol tunneling is enabled on ingress ports on a switch module, egress trunk ports forward the tunneled packets with a special encapsulation. If you also enable Layer 2 protocol tunneling on the egress trunk port, this behavior is bypassed, and the switch module forwards control PDUs without any processing or modification.
- The switch module supports LACP, and UDLD tunneling for emulated point-to-point network topologies. Protocol tunneling is disabled by default but can be enabled for the individual protocols on IEEE 802.1Q tunnel ports or on access ports.
- If you enable LACP tunneling, we recommend that you also enable UDLD on the interface for faster link-failure detection.
- Loopback detection is not supported on Layer 2 protocol tunneling of LACP or UDLD packets.
- EtherChannel port groups are compatible with tunnel ports when the IEEE 802.1Q configuration is consistent within an EtherChannel port group.
- If an encapsulated PDU (with the proprietary destination MAC address) is received from a tunnel port or an access port with Layer 2 tunneling enabled, the tunnel port is shut down to prevent loops. The port also shuts down when a configured shutdown threshold for the protocol is reached. You can manually re-enable the port (by entering a **shutdown** and a **no shutdown** command sequence). If errdisable recovery is enabled, the operation is retried after a specified time interval.
- Only decapsulated PDUs are forwarded to the customer network. The spanning-tree instance running on the service-provider network does not forward BPDUs to tunnel ports. CDP packets are not forwarded from tunnel ports.

- When protocol tunneling is enabled on an interface, you can set a per-protocol, per-port, shutdown threshold for the PDUs generated by the customer network. If the limit is exceeded, the port shuts down. You can also limit BPDU rate by using QoS ACLs and policy maps on a tunnel port.
- When protocol tunneling is enabled on an interface, you can set a per-protocol, per-port, drop threshold for the PDUs generated by the customer network. If the limit is exceeded, the port drops PDUs until the rate at which it receives them is below the drop threshold.
- Because tunneled PDUs (especially STP BPDUs) must be delivered to all remote sites so that the customer virtual network operates properly, you can give PDUs higher priority within the service-provider network than data packets received from the same tunnel port. By default, the PDUs use the same CoS value as data packets.

Configuring Layer 2 Protocol Tunneling

Beginning in privileged EXEC mode, follow these steps to configure a port for Layer 2 protocol tunneling:

	Steps	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and enter the interface to be configured as a tunnel port. This should be the edge port in the service-provider network that connects to the customer switch module. Valid interfaces can be physical interfaces and port-channel logical interfaces (port channels 1 to 48).	**interface** *interface-id*
Step 3	Configure the interface as an access port or an IEEE 802.1Q tunnel port.	**switchport mode access** or **switchport mode dot1q-tunnel**
Step 4	Enable protocol tunneling for the desired protocol. If no keyword is entered, tunneling is enabled for all three Layer 2 protocols.	**l2protocol-tunnel** [**cdp** | **stp** | **vtp**]
Step 5	(Optional) Configure the threshold for packets-per-second accepted for encapsulation. The interface is disabled if the configured threshold is exceeded. If no protocol option is specified, the threshold applies to each of the tunneled Layer 2 protocol types. The range is 1 to 4096. The default is to have no threshold configured. **Note** If you also set a drop threshold on this interface, the shutdown-threshold value must be greater than or equal to the drop-threshold value.	**l2protocol-tunnel shutdown-threshold** [**cdp** | **stp** | **vtp**] *value*

	Steps	Command
Step 6	(Optional) Configure the threshold for packets-per-second accepted for encapsulation. The interface drops packets if the configured threshold is exceeded. If no protocol option is specified, the threshold applies to each of the tunneled Layer 2 protocol types. The range is 1 to 4096. The default is to have no threshold configured. If you also set a shutdown threshold on this interface, the drop-threshold value must be less than or equal to the shutdown-threshold value.	**l2protocol-tunnel drop-threshold** [**cdp** | **stp** | **vtp**] *value*
Step 7	Return to global configuration mode.	**exit**
Step 8	(Optional) Configure the recovery mechanism from a Layer 2 maximum-rate error so that the interface is re-enabled and can try again. Errdisable recovery is disabled by default; when enabled, the default time interval is 300 seconds.	**errdisable recovery cause l2ptguard**
Step 9	(Optional) Configure the CoS value for all tunneled Layer 2 PDUs. The range is 0 to 7; the default is the default CoS value for the interface. If none is configured, the default is 5.	**l2protocol-tunnel cos** *value*
Step 10	Return to privileged EXEC mode.	**end**
Step 11	Display the Layer 2 tunnel ports on the switch module, including the protocols configured, the thresholds, and the counters.	**show l2protocol**
Step 12	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

Use the **no l2protocol-tunnel** [**cdp** | **stp** | **vtp**] interface configuration command to disable protocol tunneling for one of the Layer 2 protocols or for all three. Use the **no l2protocol-tunnel shutdown-threshold** [**cdp** | **stp** | **vtp**] and the **no l2protocol-tunnel drop-threshold** [**cdp** | **stp** | **vtp**] commands to return the shutdown and drop thresholds to the default settings.

This example shows how to configure Layer 2 protocol tunneling for CDP, STP, and VTP and to verify the configuration:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)# l2protocol-tunnel stp
Switch(config-if)# l2protocol-tunnel vtp
Switch(config-if)# l2protocol-tunnel shutdown-threshold 1500
Switch(config-if)# l2protocol-tunnel drop-threshold 1000
Switch(config-if)# exit
Switch(config)# l2protocol-tunnel cos 7
Switch(config)# end
Switch# show l2protocol
COS for Encapsulated Packets: 7
Port      Protocol  Shutdown    Drop    Encapsulation  Decapsulation  Drop
          Theshold  Threshold   Counter Counter        Counter
-------   -------- --------- --------- ------------- ------------- -------------
Fa0/8     cdp           1500      1000      2288          2282       0
```

```
stp           1500      1000       116           13        0
vtp           1500      1000         3           67        0
lacp          ----        ----       0            0        0
udld          ----        ----       0            0        0
```

Configuring Layer 2 Tunneling for EtherChannels

To configure Layer 2 point-to-point tunneling to facilitate the automatic creation of EtherChannels, you need to configure both the SP edge switch module and the customer switch module.

Configuring the SP Edge Switch Module

Beginning in privileged EXEC mode, follow these steps to configure a SP edge switch module for Layer 2 protocol tunneling for EtherChannels:

	Steps	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode, and enter the interface to be configured as a tunnel port. This should be the edge port in theservice-provider network that connects to the customer switch module. Valid interfaces are physical interfaces.	**interface** *interface-id*
Step 3	Configure the interface as an IEEE 802.1Q tunnel port.	**switchport mode dot1q-tunnel**
Step 4	(Optional) Enable point-to-point protocol tunneling for the desired protocol. If no keyword is entered, tunneling is enabled for all three protocols. **Caution** To avoid a network failure, make sure that the network is a point-to-point topology before you enable tunneling for LACP or UDLD packets.	**l2protocol-tunnel point-to-point** [**lacp** | **udld**]
Step 5	(Optional) Configure the threshold for packets-per-second accepted for encapsulation. The interface is disabled if the configured threshold is exceeded. If no protocol option is specified, the threshold applies to each of the tunneled Layer 2 protocol types. The range is 1 to 4096. The default is to have no threshold configured. **Note** If you also set a drop threshold on this interface, the shutdown-threshold value must be greater than or equal to the drop-threshold value.	**l2protocol-tunnel shutdown-threshold** [**point-to-point** [**lacp** | **udld**]] *value*

	Steps	Command
Step 6	(Optional) Configure the threshold for packets-per-second accepted for encapsulation. The interface drops packets if the configured threshold is exceeded. If no protocol option is specified, the threshold applies to each of the tunneled Layer 2 protocol types. The range is 1 to 4096. The default is to have no threshold configured. **Note** If you also set a shutdown threshold on this interface, the drop-threshold value must be less than or equal to the shutdown-threshold value.	**l2protocol-tunnel drop-threshold** [**point-to-point** [**lacp** | **udld**]] *value*
Step 7	Disable CDP on the interface.	**no cdp enable**
Step 8	Enable BPDU filtering on the interface.	**spanning-tree bpdufilter enable**
Step 9	Return to global configuration mode.	**exit**
Step 10	(Optional) Configure the recovery mechanism from a Layer 2 maximum-rate error so that the interface is re-enabled and can try again. Errdisable recovery is disabled by default; when enabled, the default time interval is 300 seconds.	**errdisable recovery cause l2ptguard**
Step 11	(Optional) Configure the CoS value for all tunneled Layer 2 PDUs. The range is 0 to 7; the default is the default CoS value for the interface. If none is configured, the default is 5.	**l2protocol-tunnel cos** *value*
Step 12	Return to privileged EXEC mode.	**end**
Step 13	Display the Layer 2 tunnel ports on the switch module, including the protocols configured, the thresholds, and the counters.	**show l2protocol**
Step 14	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

- To disable point-to-point protocol tunneling for one of the Layer 2 protocols or for all three, use the **no l2protocol-tunnel** [**point-to-point** [**lacp** | **udld**]] interface configuration command.
- To return the shutdown and drop thresholds to the default settings, use the **no l2protocol-tunnel shutdown-threshold** [**point-to-point** [**lacp** | **udld**]] and the **no l2protocol-tunnel drop-threshold** [[**point-to-point** [**lacp** | **udld**]] commands.

Configuring the Customer Switch Module

After configuring the SP edge switch module, begin in privileged EXEC mode and follow these steps to configure a customer switch module for Layer 2 protocol tunneling for EtherChannels:

	Steps	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter the interface configuration mode. This should be the customer switch module port.	**interface** *interface-id*
Step 3	Set the trunking encapsulation format to IEEE 802.1Q.	**switchport trunk encapsulation dot1q**
Step 4	Enable trunking on the interface.	**switchport mode trunk**
Step 5	Enable UDLD in **normal** mode on the interface.	**udld enable**
Step 6	Assign the interface to a channel group. For more information about configuring EtherChannels, see Chapter 15, "EtherChannel Configuration and Link State Tracking."	**channel-group** *channel-group-number* **mode desirable**
Step 7	Return to global configuration mode.	**exit**
Step 8	Enter port-channel interface mode.	**interface port-channe**l *port-channel number*
Step 9	Shut down the interface.	**shutdown**
Step 10	Enable the interface.	**no shutdown**
Step 11	Return to privileged EXEC mode.	**end**
Step 12	Display the Layer 2 tunnel ports on the switch module, including the protocols configured, the thresholds, and the counters.	**show l2protocol**
Step 13	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

Use the **no switchport mode trunk**, the **no udld enable**, and the **no channel group** *channel-group-number* **mode desirable** interface configuration commands to return the interface to the default settings.

For EtherChannels, you need to configure both the SP edge switches and the customer switches for Layer 2 protocol tunneling. (See Figure 13-6 on page 13-9.)

This example shows how to configure the SP edge switch module 1 and edge switch module 2. VLANs 17, 18, 19, and 20 are the access VLANs, Fast Ethernet interfaces 1 and 2 are point-to-point tunnel ports with UDLD enabled, the drop threshold is 1000, and Fast Ethernet interface 3 is a trunk port.

SP edge switch module 1 configuration:

```
Switch(config)# interface fastethernet1/0/1
Switch(config)# interface fastethernet0/1
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport access vlan 17
Switch(config-if)# switchport mode dot1q-tunnel
SSwitch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# exit

Switch(config)# interface fastethernet1/0/2
Switch(config)# interface fastethernet0/2
Switch(config)# interface fastethernet0/2
Switch(config-if)# switchport access vlan 18
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point udld
```

```
Switch(config-if)# exit

Switch(config)# interface fastethernet1/0/3
Switch(config)# interface fastethernet0/3
Switch(config-if)# switchport trunk encapsulation isl
Switch(config)# interface fastethernet0/9
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
```

SP edge switch module 2 configuration:

```
Switch(config)# interface fastethernet1/0/1
Switch(config)# interface fastethernet1/0/1
Switch(config)# interface fastethernet0/1
Switch(config)# interface fastethernet0/9
Switch(config-if)# switchport access vlan 19
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# exit

Switch(config)# interface fastethernet1/0/2
Switch(config)# interface fastethernet0/2
Switch(config)# interface fastethernet0/10
Switch(config-if)# switchport access vlan 20
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# exit

Switch(config)# interface fastethernet1/0/3
Switch(config)# interface fastethernet0/3
Switch(config-if)# switchport trunk encapsulation isl
Switch(config)# interface fastethernet0/11
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
```

This example shows how to configure the customer switch module at Site 1. Fast Ethernet interfaces 1, 2, 3, and 4 are set for IEEE 802.1Q trunking, UDLD is enabled, EtherChannel group 1 is enabled, and the port channel is shut down and then enabled to activate the EtherChannel configuration:

```
Switch(config)# interface fastethernet1/0/1
Switch(config)# interface fastethernet0/1
Switch(config)# interface fastethernet0/9
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit

Switch(config)# interface fastethernet1/0/2
Switch(config)# interface fastethernet0/2
Switch(config)# interface fastethernet0/10
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit

Switch(config)# interface fastethernet1/0/3
Switch(config)# interface fastethernet0/3
Switch(config)# interface fastethernet0/11
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
```

```
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit

Switch(config)# interface fastethernet1/0/4
Switch(config)# interface fastethernet0/4
Switch(config)# interface fastethernet0/12
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# udld enable
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# exit
Switch(config)# interface port-channel 1
Switch(config-if)# shutdown
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

Monitoring and Maintaining Tunneling Status

Table 13-2 shows the privileged EXEC commands for monitoring and maintaining IEEE 802.1Q and Layer 2 protocol tunneling.

Table 13-2 Commands for Monitoring and Maintaining Tunneling

Descriptions	Command
Clear the protocol counters on Layer 2 protocol tunneling ports.	**clear l2protocol-tunnel counters**
Display IEEE 802.1Q tunnel ports on the switch module.	**show dot1q-tunnel**
Verify if a specific interface is a tunnel port.	**show dot1q-tunnel interface** *interface-id*
Display information about Layer 2 protocol tunneling ports.	**show l2protocol-tunnel**
Verify if the recovery timer from a Layer 2 protocol-tunnel error disable state is enabled.	**show errdisable recovery**
Display information about a specific Layer 2 protocol tunneling port.	**show l2protocol-tunnel interface** *interface-id*
Display only Layer 2 protocol summary information.	**show l2protocol-tunnel summary**
Display the status of native VLAN tagging on the switch module.	**show vlan dot1q tag native**

For detailed information about these displays, see the command reference for this release.

Quality of Service Configuration

This chapter describes how to configure Quality of Service (QoS) by using the modular QoS Command Line Interface (CLI), or MQC, commands on the CGR 2010 ESM. With QoS, you can provide preferential treatment to certain types of traffic at the expense of others. When QoS is not configured, the switch module offers best-effort service to each packet, regardless of the packet contents or size. It sends the packets without any assurance of reliability, delay bounds, or throughput. MQC provides a comprehensive hierarchical configuration framework for prioritizing or limiting specific streams of traffic.

This chapter also describes QoS features for implementing high-priority (low-latency) traffic via the internal data path between the CGR 2010 ESM and the host Cisco CGR 2010 router. The internal data path is called *PortChannel48 (see "Implementing High-Priority Traffic to the Host Router" section on page 14-95)*. For more information, see also Chapter 9, "EtherChannel Configuration Between the Switch Module and the Host Router."

Note IPv6 QoS is not supported.

For more information about Cisco IOS MQC commands, see the "Cisco IOS Quality of Service Solutions Command Reference" at this site:

http://www.cisco.com/en/US/docs/ios/12_2/qos/command/reference/fqos_r.html

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

For information about using Ethernet terminal loopback to test full-path QoS on an interface, see the "Enabling Ethernet Loopback" section in Chapter 45, "Configuring Ethernet OAM, CFM, and E-LMI" in the *Cisco CGS 2520 Software Configuration Guide*.

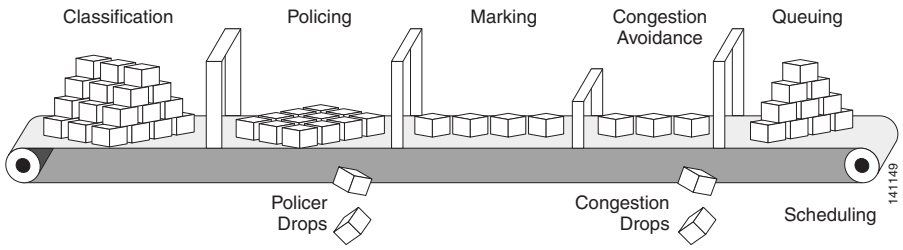
Understanding QoS

Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

When you configure the QoS feature, you can select specific network traffic, prioritize it according to its relative importance, and use traffic-management techniques to provide preferential treatment. Implementing QoS in your network makes network performance more predictable and bandwidth utilization more effective.

Figure 14-1 shows the Modular QoS CLI (MQC) model.

Figure 14-1 Modular QoS CLI Model



Basic QoS includes these actions.

- *Packet classification* organizes traffic on the basis of whether or not the traffic matches a specific criteria. When a packet is received, the switch module identifies all key packet fields: class of service (CoS), Differentiated Services Code Point (DSCP), or IP precedence. The switch module classifies the packet based on this content or based on an access-control list lookup. For more information, see the "Classification" section on page 14-6.
- *Packet policing* determines whether a packet is in or out of profile by comparing the rate of the incoming traffic to the configured policer. Packet policing determines whether a packet is in or out of profile by comparing the rate of the incoming traffic to the configured policer. You can control the traffic flow for packets that conform to or exceed the configured policer. You can configure a committed information rate (CIR) and peak information rate (PIR) and set actions to perform on packets that conform to the CIR and PIR (conform-action), packets that conform to the PIR, but not the CIR (exceed-action), and packets that exceed the PIR value (violate-action). For more information, see the "Policing" section on page 14-15.
- *Packet prioritization or marking* evaluates the classification and policer information to determine the action to take. All packets that belong to a classification can be remarked. When you configure a policer, packets that meet or exceed the permitted bandwidth requirements (bits per second) can be conditionally passed through, dropped, or reclassified. For more information, see the "Marking" section on page 14-21.
- *Congestion management* uses queuing and scheduling algorithms to queue and sort traffic that is leaving a port. The switch module supports these scheduling and traffic-limiting features: class-based weighted fair queuing (CBWFQ), class-based traffic shaping, port shaping, and class-based priority queuing. You can provide guaranteed bandwidth to a particular class of traffic while still servicing other traffic queues. For more information, see the "Congestion Management and Scheduling" section on page 14-26.
- *Weighted tail-drop (WTD).* Queuing on the switch module is enhanced with the weighted tail-drop (WTD) algorithm, a congestion-avoidance mechanism. WTD differentiates traffic classes and regulates the queue size (in number of packets) based on the classification. For more information, see the "Congestion Avoidance and Queuing" section on page 14-32.

This section includes information about these topics:

Modular QoS CLI

Modular QoS CLI (MQC) allows users to create traffic policies and attach these policies to interfaces. A traffic policy contains a traffic class and one or more QoS features. You use a traffic class to classify traffic, and the QoS features in the traffic policy determine how to treat the classified traffic.

Modular QoS CLI configuration includes these steps:

Step 1 Define a traffic class.

Use the **class-map** [**match-all** | **match-any**] *class-map-name* global configuration command to define a traffic class and to enter class-map configuration mode. A traffic class contains three elements: a name, an instruction on how to evaluate the configured **match** commands (if more than one match command is configured in the class map), and a series of **match** commands

- You name the traffic class in the **class-map** command line to enter class-map configuration mode.
- You can optionally include keywords to evaluate these match commands by entering **class-map match-any** or **class-map match-all**. If you specify **match-any**, the traffic being evaluated must match *one* of the specified criteria. If you specify **match-all**, the traffic being evaluated must match *all* of the specified criteria. A **match-all** class map can contain only one match statement, but a **match-any** class map can contain multiple match statements.

  Note If you do not enter **match-all** or **match-any**, the default is to match all.

- You use the **match** class-map configuration commands to specify criteria for classifying packets. If a packet matches the specified criteria, that packet is considered a member of the class and is forwarded according to the QoS specifications set in the traffic policy. Packets that fail to meet any of the matching criteria are classified as members of the default traffic class.

Step 2 Create a traffic policy to associate the traffic class with one or more QoS features.

You use the **policy-map** *policy-map-name* global configuration command to create a traffic policy and to enter policy-map configuration mode. A traffic policy defines the QoS features to associate with the specified traffic class. A traffic policy contains three elements: a name, a traffic class (specified with the **class** policy-map configuration command), and the QoS policies configured in the class.

- You name the traffic policy in the **policy-map** command line to enter policy-map configuration mode.

- In policy-map configuration mode, enter the name of the traffic class used to classify traffic to the specified policy, and enter policy-map class configuration mode.
- In policy-map class configuration mode, you can enter the QoS features to apply to the classified traffic. These include using the **set**, **police**, or **police aggregate** commands for input policy maps or the **bandwidth**, **priority**, **queue-limit** or **shape average** commands for output policy maps.

Note A packet can match only one traffic class within a traffic policy. If a packet matches more than one traffic class in the traffic policy, the first traffic class defined in the policy is used. To configure more than one match criterion for packets, you can associate multiple traffic classes with a single traffic policy.

Step 3 Attach the traffic policy to an interface.

You use the **service-policy** interface configuration command to attach the policy map to an interface for packets entering or leaving the interface. You must specify whether the traffic policy characteristics should be applied to incoming or outgoing packets. For example, entering the **service-policy output class1** interface configuration command attaches all the characteristics of the traffic policy named *class1* to the specified interface. All packets leaving the specified interface are evaluated according to the criteria specified in the traffic policy named *class1*.

Note If you enter the **no** policy-map configuration command or the **no policy-map** *policy-map-name* global configuration command to delete a policy map that is attached to an interface, a warning message appears that lists any interfaces from which the policy map is being detached. The policy map is then detached and deleted. For example:

```
Warning: Detaching Policy test1 from Interface GigabitEthernet0/1
```

Input and Output Policies

Policy maps are either input policy maps or output policy maps, attached to packets as they enter or leave the switch module by service policies applied to interfaces. Input policy maps perform policing and marking on received traffic. Policed packets can be dropped or reduced in priority (marked down) if they exceed the maximum permitted rates. Output policy maps perform scheduling and queuing on traffic as it leaves the switch module.

Input policies and output policies have the same basic structure; the difference is in the characteristics that they regulate. Figure 14-2 shows the relationship of input and output policies.

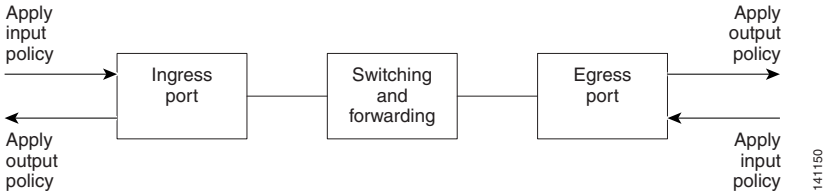
The number of configurable policer profiles on the switch module is 256. The number of supported policer instances on the switch module is 1,024 minus 1 more than the number of interfaces on the switch module.

The number of policer instances for the Copper model (GRWIC-D-ES-2S-8PC), which has ten interfaces, is 1,013; the number of policer instances for the SFP model (GRWIC-D-ES-6S), which has six interfaces, is 1,017.

- You can use a policer profile in multiple instances
- You can configure a maximum of 256 policy maps
- You can apply one input policy map and one output policy map to an interface.

When CPU protection is enabled (the default), you can configure 45 ingress policers per port. If you disable CPU protection by entering the **no policer cpu uni all** global configuration command and reloading the switch module, you can configure a maximum of 63 policers per port for user-defined classes and one for class-default. You can enter the **show policer cpu uni-eni** {**drop** | **rate**} privileged EXEC command to see if CPU protection is enabled.

Figure 14-2 Input and Output Policy Relationship



Input Policy Maps

Input policy map classification criteria include matching a CoS, a DSCP, or an IP precedence value or matching an access control list (ACL) or VLAN ID (for per-port, per-VLAN QoS). Input policy maps can have any of these actions:

- Setting or marking a CoS, a DSCP, an IP precedence, or QoS group value
- Individual policing
- Aggregate policing

Only input policies provide matching on access groups or VLAN IDs, and only output policies provide matching on QoS groups. You can assign a QoS group number in an input policy and match it in the output policy. The class **class-default** is used in a policy map for any traffic that does not explicitly match any other class in the policy map. Input policy maps do not support queuing and scheduling keywords, such as **bandwidth**, **queue-limit**, **priority**, and **shape average**.

An input policy map can have a maximum of 64 classes plus **class-default**. You can configure a maximum of 64 classes in an input policy.

Output Policy Maps

Output policy map classification criteria include matching a CoS, a DSCP, an IP precedence, or a QoS group value. Output policy maps can have any of these actions:

- Queuing (**queue-limit**)
- Scheduling (**bandwidth**, **priority**, and **shape average**)

Output policy maps do not support matching of access groups. You can use QoS groups as an alternative by matching the appropriate access group in the input policy map and setting a QoS group. In the output policy map, you can then match the QoS group. See the "Classification Based on QoS Groups" section on page 14-12 for more information.

Output policies do not support marking or policing (except in the case of priority with policing). There is no egress packet marking on the switch module (no **set** command in an output policy).

The class **class-default** is used in a policy map for any traffic that does not explicitly match any other class in the policy map. There can be a maximum of four classes in the output policy map (including class-default) because egress ports have a maximum of four queues.

An output policy map attached to an egress port can match only the packets that have already been matched by an input policy map attached to the ingress port for the packets. You can attach an output policy map to any or all ports on the switch module. The switch module supports configuration and attachment of a unique output policy map for each port. However, these output policy maps can contain only three unique configurations of queue limits. These three unique queue-limit configurations can be included in as many output policy maps as there are ports on the switch module. There are no limitations on the configurations of bandwidth, priority, or shaping.

You can configure the output policy classification criteria for CPU-generated traffic by using the **cpu traffic qos** [**cos** *value* | **dscp** *value* | **precedence** *value* | **qos-group** *value*] global configuration command.

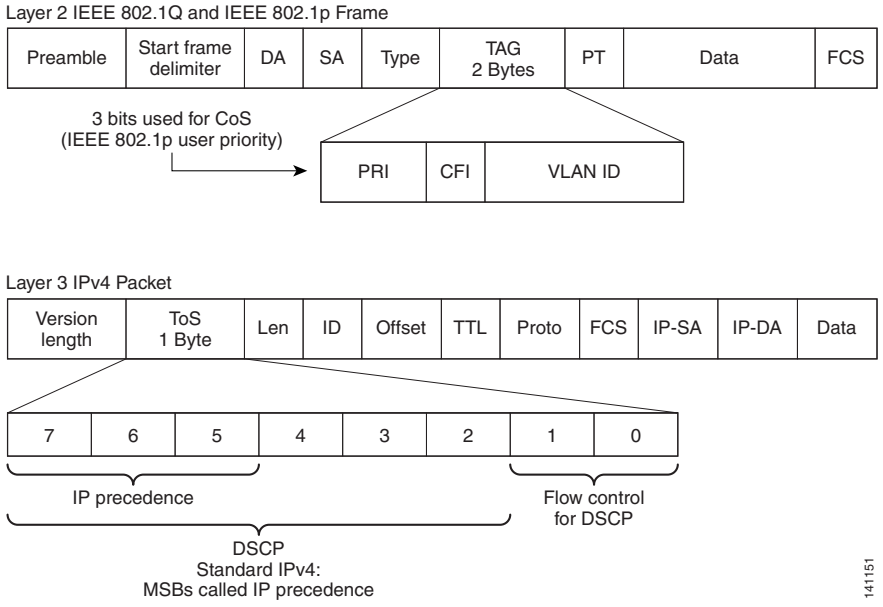
Classification

Classification distinguishes one kind of traffic from another by examining the fields in the packet header. When a packet is received, the switch module examines the header and identifies all key packet fields. A packet can be classified based on an ACL, on the DSCP, the CoS, or the IP precedence value in the packet, or by the VLAN ID. Figure 14-3 has examples of classification information carried in a Layer 2 or a Layer 3 IP packet header, using six bits from the deprecated IP type of service (ToS) field to carry the classification information.

- On ports configured as Layer 2 IEEE 802.1Q trunks, all traffic is in 802.1Q frames except for traffic in the native VLAN. Layer 2 802.1Q frame headers have a 2-byte Tag Control Information field that carries the CoS value, called the User Priority bits, in the three most-significant bits, and the VLAN ID value in the 12 least-significant bits. Other frame types cannot carry Layer 2 CoS values.
- Layer 2 CoS values range from 0 to 7.
- Layer 3 IP packets can carry either an IP precedence value or a DSCP value. QoS supports the use of either value because DSCP values are backward-compatible with IP precedence values.

  IP precedence values range from 0 to 7. DSCP values range from 0 to 63.
- Output remarking is based on the Layer 2 or Layer 3 marking type, marking value and packet type.

Figure 14-3 QoS Classification Layers in Frames and Packets



These sections contain additional information about classification:

Class Maps

As explained previously, you use an MQC class map to name a specific traffic flow (or class) and to isolate it from all other traffic. A class map defines the criteria used to match against a specific traffic flow to further classify it. If you have more than one type of traffic that you want to classify, you can create another class map and use a different name. When you enter the **class-map** command with a class-map name, the switch module enters the class-map configuration mode. In this mode, you define the match criterion for the traffic by using the **match** class-map configuration command. After a packet is matched against the class-map criteria, it is acted on by the associated action specified in a policy map.

You can match more than one criterion for classification. You can also create a class map that requires that all matching criteria in the class map be in the packet header by using the **class map match-all** *class-map name* global configuration command to enter class map configuration mode.

Note You can configure only one match entry in a **match-all** class map.

You can use the **class map match-any** *class-map name* global configuration command to define a classification with any of the listed criteria.

Note If you do not enter **match-all** or **match-any**, the default is to match all. A match-all class map cannot have more than one classification criterion (match statement). A class map with no match condition has a default of **match all**.

The *match* Command

To configure the type of content used to classify packets, you use the **match** class-map configuration command to specify the classification criteria. If a packet matches the configured criteria, it belongs to a specific class and is forwarded according to the specified policy. For example, you can use the **match** class-map command with CoS, IP DSCP, and IP precedence values. These values are referred to as *markings* on a packet. You can also match an access group, a QoS group, or a VLAN ID or ID range for per-port, per-VLAN QoS.

- For an input policy map, you cannot configure an IP classification (**match ip dscp**, **match ip precedence**, **match access-group** for an IP ACL) and a non-IP classification (**match cos** or **match access-group** for a MAC ACL) in the same policy map or class map.

- When an input policy map with only Layer 2 classification is attached to a routed port or a switch module port containing a routed switch module virtual interface (SVI), the service policy acts only on switching eligible traffic and not on routing eligible traffic.
- On an 802.1Q tunnel port, you can use only an input policy map with Layer 2 classification based on MAC ACLs to classify traffic. Input policy maps with Layer 3 classification, match Layer 2 CoS classification, or per-port, per-VLAN policies are not supported on tunnel ports.
- In an output policy map, no two class maps can have the same classification criteria, that is, the same match qualifiers and values.

This example shows how to create a class map *example* to define a class that matches any of the listed criteria. In this example, if a packet is received with the DSCP equal to 32 or a 40, the packet is identified (classified) by the class map:

```
Switch(config)# class-map match-any example
Switch(config-cmap)# match ip dscp 32
Switch(config-cmap)# match ip dscp 40
Switch(config-cmap)# exit
```

Classification Based on Layer 2 CoS

You can use the **match** command to classify Layer 2 traffic based on the CoS value, which ranges from 0 to 7.

Note A **match cos** command is supported only on Layer 2 802.1Q trunk ports.

This example shows how to create a class map to match a CoS value of 5:

```
Switch(config)# class-map premium
Switch(config-cmap)# match cos 5
Switch(config-cmap)# exit
```

Classification Based on IP Precedence

You can classify IPv4 traffic based on the packet IP precedence values, which range from 0 to 7. This example shows how to create a class map to match an IP precedence value of 4:

```
Switch(config)# class-map sample
Switch(config-cmap)# match ip precedence 4
Switch(config-cmap)# exit
```

Classification Based on IP DSCP

When you classify IPv4 traffic based on IP DSCP value, and enter the **match ip dscp** class-map configuration command, you have several classification options:

- Entering a specific DSCP value (0 to 63).
- Using the Default service, which corresponds to an IP precedence and DSCP value of 0. The default per-hop behavior (PHB) is usually best-effort service.

- Using Assured Forwarding (AF) by entering the binary representation of the DSCP value. AF sets the relative probability that a specific class of packets is forwarded when congestion occurs and the traffic does not exceed the maximum permitted rate. AF *per-hop behavior* provides delivery of IP packets in four different AF classes: AF11-13 (the highest), AF21-23, AF31-33, and AF41-43 (the lowest). Each AF class could be allocated a specific amount of buffer space and drop probabilities, specified by the binary form of the DSCP number. When congestion occurs, the drop precedence of a packet determines the relative importance of the packet within the class. An AF41 provides the best probability of a packet being forwarded from one end of the network to the other.
- Entering Class Selector (CS) service values of 1 to 7, corresponding to IP precedence bits in the ToS field of the packet.
- Using Expedited Forwarding (EF) to specify a low-latency path. This corresponds to a DSCP value of 46. EF services use priority queuing to preempt lower priority traffic classes.

This display shows the available classification options:

```
Switch(config-cmap)# match ip dscp ?
  <0-63>   Differentiated services codepoint value
  af11     Match packets with AF11 dscp (001010)
  af12     Match packets with AF12 dscp (001100)
  af13     Match packets with AF13 dscp (001110)
  af21     Match packets with AF21 dscp (010010)
  af22     Match packets with AF22 dscp (010100)
  af23     Match packets with AF23 dscp (010110)
  af31     Match packets with AF31 dscp (011010)
  af32     Match packets with AF32 dscp (011100)
  af33     Match packets with AF33 dscp (011110)
  af41     Match packets with AF41 dscp (100010)
  af42     Match packets with AF42 dscp (100100)
  af43     Match packets with AF43 dscp (100110)
  cs1      Match packets with CS1(precedence 1) dscp (001000)
  cs2      Match packets with CS2(precedence 2) dscp (010000)
  cs3      Match packets with CS3(precedence 3) dscp (011000)
  cs4      Match packets with CS4(precedence 4) dscp (100000)
  cs5      Match packets with CS5(precedence 5) dscp (101000)
  cs6      Match packets with CS6(precedence 6) dscp (110000)
  cs7      Match packets with CS7(precedence 7) dscp (111000)
  default  Match packets with default dscp (000000)
  ef       Match packets with EF dscp (101110)
```

For more information on DSCP prioritization, see RFC-2597 (AF per-hop behavior), RFC-2598 (EF), or RFC-2475 (DSCP).

802.1Q Tunneling CoS Mapping

The switch module supports VLAN mapping from the customer VLAN-ID (C-VLAN) to a service-provider VLAN-ID (S-VLAN). See the

"Understanding VLANs" section on page 11-1. For QoS, the switch module can set the service-provider CoS (S-CoS) from either the customer CoS (C-CoS) or the customer DSCP (C-DSCP) value, and can map the inner CoS to the outer CoS for any traffic with traditional 802.1Q tunneling (QinQ) or selective QinQ VLAN mapping. This default allows copying the customer CoS into the service provider network.

The switch module supports C-CoS to S-CoS propagation for traditional QinQ and for selective QinQ on trunk ports. This is the default behavior and does not require configuration. When you configure traditional QinQ or selective QinQ on Layer 2 trunk ports using 1-to-2 VLAN mapping, the switch module also allows setting the S-CoS from C-DSCP.

For traffic entering the switch module on 802.1Q tunnel ports or trunk ports configured for VLAN mapping, the switch module has the ability to examine the customer packet header and set the service-provider CoS value (S-CoS) from either the customer CoS value or the customer DSCP value.

Configuring CoS matching on 802.1Q mapped ports is handled in this way:

- On interfaces configured for 802.1Q tunneling (on tunnel or trunk ports) or selective 802.1Q (on trunk ports), the CoS value of the VLAN tag (inner VLAN or C-VLAN) received on the interface (C-CoS) is automatically reflected in the tunnel VLAN tag (outer VLAN or S-VLAN) by default.
- The **set cos** policy-map class configuration commands always apply to the outer-most VLAN tag after processing is complete, that is the S-VLAN-ID. For example, in 802.1Q tunnels, entering a **set cos** command changes only the CoS value of the outer tag of the encapsulated packet.
- When you configure a policy by entering the **match dscp** class map configuration command and you enter the **set cos** policy-map class configuration command for QinQ and selective QinQ mapping interfaces, a DSCP match sets the outer CoS of the encapsulated value.
- You can set DSCP based on matching the outer VLAN.
- If you enter the **match cos** command on interfaces configured for traditional QinQ or for selective QinQ mapping, the match is to the outer CoS, which is the reflected inner Cos (C-CoS).

Classification Comparisons

Table 14-1 shows suggested IP DSCP, IP precedence, and CoS values for typical traffic types.

Table 14-1 Typical Traffic Classifications

Traffic Type	DSCP per-hop	DSCP (decimal)	IP Precedence	CoS
Voice-bearer—traffic in a priority queue or the queue with the highest service weight and lowest drop priority.	EF	46	5	5
Voice control—signalling traffic, related to call setup, from a voice gateway or a voice application server.	AF31	26	3	3
Video conferencing—in most networks, video conferencing over IP has similar loss, delay, and delay variation requirements as voice over IP traffic.	AF41	34	4	4
Streaming video—relatively high bandwidth applications with a high tolerance for loss, delay, and delay variation. Usually considered more important than regular background applications such as e-mail and web browsing.	AF13	14	1	1
Mission critical date (gold data)—delay-sensitive applications critical to the operation of an enterprise. Level 1 Level 2 Level 3	 AF21 AF22 AF23	 18 20 22	 2 2 2	 2 2 2

Table 14-1 Typical Traffic Classifications (continued)

Traffic Type	DSCP per-hop	DSCP (decimal)	IP Precedence	CoS
Less critical data (silver data)—noncritical, but relatively important data.				
Level 1	AF11	10	1	1
Level 2	AF12	12	1	1
Level 3	AF13	14	1	1
Best-effort data (bronze data)—other traffic, including all noninteractive traffic, regardless of importance.	Default	0	0	0
Less than best-effort data—noncritical, bandwidth-intensive data traffic given the least preference. This is the first traffic type to be dropped.		2	0	0
Level 1		4	0	0
Level 2		6	0	0
Level 3				

Classification Based on QoS ACLs

Packets can also be classified in input policy maps based on an ACL lookup. The ACL classification is communicated to an output policy by assigning a QoS group or number in the input policy map. To classify based on ACL lookup, you first create an IP or MAC ACL. Configure a class map and use the **match access-group** {*acl-number* | *acl name*} class-map configuration command, and attach the class map to a policy map.

Note You cannot configure **match access-group** for an output policy map.

You can use IP standard, IP extended, or Layer 2 MAC ACLs to define a group of packets with the same characteristics (a class). You use the **access-list** global configuration command to configure IP ACLS to classify IP traffic based on Layer 3 and Layer 4 parameters. You use the **mac access-list extended** global configuration command to configure Layer 2 MAC ACLs to classify IP and non-IP traffic based on Layer 2 parameters.

Note You cannot match IP fragments against configured IP extended ACLs to enforce QoS. IP fragments are sent as best-effort. IP fragments are denoted by fields in the IP header.

You can use only ACLs with a permit action in a **match access-group** command. ACLs with a deny action are never matched in a QoS policy.

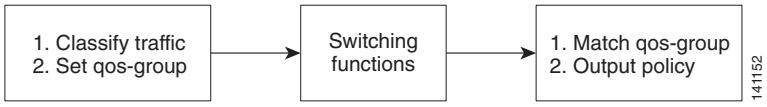
Note Only one access-group is supported per class for an input policy map.

Classification Based on QoS Groups

A QoS group is an internal label used by the switch module to identify packets as a members of a specific class. The label is not part of the packet header and is restricted to the switch module that sets the label. QoS groups provide a way to tag a packet for subsequent QoS action without explicitly marking (changing) the packet. You can then communicate an ACL match from an input policy map to an output policy map.

A QoS group is identified at ingress and used at egress; it is assigned in an input policy to identify packets in an output policy (see Figure 14-4). The QoS groups help aggregate different classes of input traffic for a specific action in an output policy.

Figure 14-4 QoS Groups



You can use QoS groups to aggregate multiple input streams across input classes and policy maps for the same QoS treatment on the egress port. Assign the same QoS group number in the input policy map to all streams that require the same egress treatment, and match to the QoS group number in the output policy map to specify the required queuing and scheduling actions.

You can also use QoS groups to identify traffic entering a particular interface if the traffic must be treated differently at the output based on the input interface.

You can use QoS groups to configure per-port, per-VLAN QoS output policies on the egress interface for bridged traffic on the VLAN. Assign a QoS group number to a VLAN on the ingress interface by configuring a per-port, per-VLAN input policy. Then use the same QoS-group number for classification at the egress. Because the VLAN of bridged traffic does not change during forwarding through the switch module, the QoS-group number assigned to the ingress VLAN can be used on the egress interface to identify the same VLAN.

You can use the **cpu traffic qos** [**cos** *value* | **dscp** *value* | **precedence** *value* | **qos-group** *value*] global configuration command to configure a QoS group number for CPU-generated traffic.

Independently you can assign QoS-group numbers at the ingress to any combination of interfaces, VLANs, traffic flows, and aggregated traffic. To assign QoS-group numbers, configure a QoS group marking in an input policy map, along with any other marking or policing actions required in the input policy map for the same service class. This allows the input marking and policing functions to be decoupled from the egress classification function if necessary because only the QoS group must be used for egress classification.

To communicate an ACL classification to an output policy, you assign a QoS number to specify packets at ingress. This example identifies specific packets as part of QoS group 1 for later processing in an output policy:

```
Switch(config)# policy-map in-gold-policy
Switch(config-pmap)# class in-class1
Switch(config-pmap-c)# set qos-group 1
Switch(config-cmap-c)# exit
Switch(config-cmap)# exit
```

You use the **set qos-group** command only in an input policy. The assigned QoS group identification is subsequently used in an output policy with no mark or change to the packet. You use the **match qos-group** in the output policy.

Note You cannot configure **match qos-group** for an input policy map.

This example creates an output policy to match the QoS group created in the input policy map *in-gold-policy*. Traffic internally tagged as *qos-group 1* is identified and processed by the output policy:

```
Switch(config)# class-map out-class1
Switch(config-cmap)# match qos-group 1
Switch(config-cmap)# exit
```

The switch module supports a maximum of 100 QoS groups.

Classification Based on VLAN IDs

With classification based on VLAN IDs, you can apply QoS policies to frames carried on a user-specified VLAN for a given interface. You can use hierarchical policy maps for per-VLAN classification on trunk ports. Per-VLAN classification is not required on access ports because access ports carry traffic for a single VLAN. If you try to attach an input per-port, per VLAN hierarchical policy to a port that is not a trunk port, the configuration is rejected.

The switch module supports two policy levels: a *parent* level and a *child* level. With the QoS parent-child structure, you can reference a child policy in a parent policy to provide additional control of a specific traffic type. For per-port, per-VLAN QoS, the parent-level class map specifies only the VLAN match criteria, and the child-level class maps provide more detailed classification for frames matching the parent-level class map.You can configure multiple service classes at the parent level to match different combinations of VLANs, and you can apply independent QoS policies to each parent service class using any child policy map.

Note A per-port, per-VLAN parent-level class map supports only a child-policy association; it does not allow any actions to be configured. In addition, for a parent-level class map, you cannot configure an action or a child-policy association for the class **class-default**.

Per-port, per-VLAN QoS has these limitations:

- You can apply a per-port, per-VLAN hierarchical policy map only to trunk ports.
- You can configure classification based on VLAN ID only in the parent level of a per-port, per-VLAN hierarchical policy map.
- When the child policy map attached to a VLAN or set of VLANs contains only Layer 3 classification (**match ip dscp**, **match ip precedence**, **match IP ACL**), you must be careful to ensure that these VLANs are not carried on any port other than the one on which this per-port, per-VLAN policy is attached. Not following this restriction could result in improper QoS behavior for traffic ingressing the switch module on these VLANs.
- We also recommend that you restrict VLAN membership on the trunk ports to which the per-port, per-VLAN is applied by using the **switchport trunk allowed vlan** interface configuration command. Overlapping VLAN membership between trunk ports that have per-port, per-VLAN policies with Layer 3 classification could also result in unexpected QoS behavior.

In this example, the class maps in the child-level policy map specify matching criteria for voice, data, and video traffic, and the child policy map sets the action for input policing each type of traffic. The parent-level policy map specifies the VLANs to which the child policy maps are applied on the specified port:

```
Switch(config)# class-map match-any dscp-1 data
Switch(config-cmap)# match ip dscp 1
Switch(config-cmap)# exit
Switch(config)# class-map match-any dscp-23 video
Switch(config-cmap)# match ip dscp 23
Switch(config-cmap)# exit
Switch(config)# class-map match-any dscp-63 voice
Switch(config-cmap)# match ip dscp-63
Switch(config-cmap)# exit
Switch(config)# class-map match-any customer-1-vlan
Switch(config-cmap)# match vlan 100
Switch(config-cmap)# match vlan 200
Switch(config-cmap)# match vlan 300
Switch(config-cmap)# exit
```

Note You can also enter the match criteria as **match vlan 100 200 300** with the same result.

```
Switch(config)# policy-map child policy-1
Switch(config-pmap)# class dscp-63 voice
Switch(config-pmap-c)# police cir 10000000 bc 50000
Switch(config-pmap-c)# conform-action set-cos-transmit 5
Switch(config-pmap-c)# exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# class dscp-1 data
Switch(config-pmap-c)# set cos 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# class dscp-23 video
Switch(config-pmap-c)# set cos 4
Switch(config-pmap-c)# set ip precedence 4
Switch(config-pmap-c)# exit

Switch(config)# policy-map parent-customer-1
Switch(config-pmap)# class customer-1-vlan
Switch(config-pmap-c)# service-policy ingress-policy-1
Switch(config-pmap-c)# exit

Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# service-policy input customer-1-ingress
Switch(config-pmap-c)# exit
```

Note Each per-port, per-VLAN parent policy class, except **class-default**, can have a child policy association.

See the "Configuring Per-Port Per-VLAN QoS with Hierarchical Input Policy Maps" section on page 14-59 for configuration information, including configuration guidelines and limitations.

Table Maps

You can use table maps to manage a large number of traffic flows with a single command. You can specify table maps in **set** commands and use them as mark-down mapping for the policers. You can also use table maps to map an incoming QoS marking to a replacement marking without having to configure a large number of explicit matches and sets. Table maps are used only in input policy maps.

Table maps can be used to:

- Correlate specific CoS, DSCP, or IP precedence values to specific CoS, DSCP, or IP precedence values
- Mark down a CoS, DSCP, or IP precedence value
- Assign defaults for unmapped values

A table map includes one of these default actions:

- **default** *default-value*—Applies a specific default value (0 to 63) for all unmapped values
- **default copy**—Maps all unmapped values to the equivalent value in another qualifier
- **default ignore**—Makes no changes for unmapped values

This example creates a table to map specific CoS values to DSCP values. The **default** command maps all unmapped CoS values to a DSCP value of 63.

```
Switch(config)# table-map cos-dscp-tablemap
Switch(config-tablemap)# map from 5 to 46
Switch(config-tablemap)# map from 6 to 56
Switch(config-tablemap)# map from 7 to 57
Switch(config-tablemap)# default 63
Switch(config-tablemap)# exit
```

The switch module supports a maximum of 256 unique table maps. You can enter up to 64 different **map from**–**to** entries in a table map. These table maps are supported on the switch module:

- DSCP to CoS
- DSCP to precedence
- DSCP to DSCP
- CoS to DSCP
- CoS to precedence
- CoS to CoS
- Precedence to CoS
- Precedence to DSCP
- Precedence to precedence

Table maps modify only one parameter (CoS, IP precedence, or DSCP, whichever is configured) and are only effective when configured with a **set** command in a policy map or police function. Individual policers also support the **violate-action** command, but aggregate policers do not support table maps with **violate-action**.

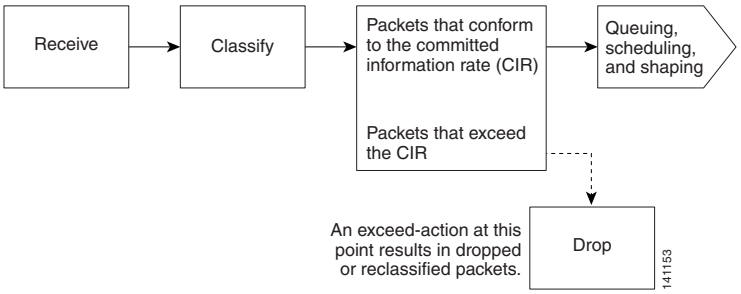
Table maps are not supported in output policy maps.

Policing

After a packet is classified, you can use policing as shown in Figure 14-5 to regulate the class of traffic. The policing function limits the amount of bandwidth available to a specific traffic flow or prevents a traffic type from using excessive bandwidth and system resources. A policer identifies a packet as in or out of profile by comparing the rate of the inbound traffic to the configuration profile of the policer and traffic class. Packets that exceed the permitted average rate or burst rate are *out of profile* or *nonconforming* These packets are dropped or modified (marked for further processing), depending on the policer configuration.

Policing is used primarily on receiving interfaces. You can attach a policy map with a policer only in an input service policy. The only policing allowed in an output policy map is in priority classes. See the "Unconditional Priority Policing" section on page 14-20.

Figure 14-5 Policing of Classified Packets



These sections describe the types of policing supported on the switch module:

- Individual Policing, page 14-16
- Aggregate Policing, page 14-18
- Unconditional Priority Policing, page 14-20

Individual Policing

Individual policing applies only to input policy maps. In policy-map configuration mode, you enter the **class** command followed by class-map name, and enter policy-map class configuration mode.

The switch module supports 1-rate, 2-color ingress policing and 2-rate, 3-color policing for individual or aggregate policing.

For 1-rate, 2-color policing, you use the **police** policy-map class configuration command to define the policer, the committed rate limitations of the traffic, committed burst size limitations of the traffic, and the action to take for a class of traffic that is below the limits (**conform-action**) and above the limits (**exceed-action**). If you do not specify burst size (bc), the system calculates an appropriate burst size value. The calculated value is appropriate for most applications. For more information, see the "Attaching a Traffic Policy to an Interface" section on page 14-47.

When you configure a 2-rate policer, in addition to configuring the committed information rate (CIR) for updating the first token bucket, you also configure the peak information rate (PIR) at which the second token bucket is updated. If you do not configure a PIR, the policer is a standard 1-rate, 2-color policer.

For 2-rate, 3-color policing, you can then optionally set actions to perform on packets that conform to the specified CIR and PIR (conform-action), packets that conform to the PIR, but not the CIR (exceed-action), and packets that exceed the PIR value (violate-action).

- If you set the CIR value equal to the PIR, a traffic rate that is less than or equal to the CIR is in the conform range. Traffic that exceeds the CIR is in the violate range.
- If you set the PIR greater than the CIR, a traffic rate less than the CIR is in the conform range. A traffic rate that exceeds the CIR but is less than or equal to the PIR is in the exceed range. A traffic rate that exceeds the PIR is in the violate range.
- If you do not configure a PIR, the policer is configured as a 1-rate, 2-color policer.

Setting the burst sizes too low can reduce throughput in situations with bursty traffic. Setting burst sizes too high can allow too high a traffic rate.

Note The switch module supports byte counters for byte-level statistics for conform, exceed, and violate classes in the show policy-map interface privileged EXEC command output.

To make the policy map effective, you attach it to a physical port by using the **service-policy input** interface configuration command. Policing is done only on received traffic, so you can only attach a policer to an input service policy.

This is an example of basic policing for all traffic received with a CoS of 4. The first value following the **police** command limits the average traffic rate to 10, 000,000 bits per second (bps); the second value represents the additional burst size (10 kilobytes). The policy is assigned to Fast Ethernet port 1:

```
Switch(config)# table-map cos-dscp-tablemap
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map video-policy
Switch(config-pmap)# class video-class
Switch(config-pmap-c)# police 10000000 10000
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input video-policy
Switch(config-if)# exit
```

You can use the **conform-action**, **exceed-action**, and **violate-action** policy-map class configuration commands or the **conform-action**, **exceed-action**, and **violate-action** policy-map class police configuration commands to specify the action to be taken when the packet conforms to or exceeds the specified traffic rates. Conform, exceed, and violate actions are to drop the packet, to send the packet without modifications, to set a new CoS, DSCP, or IP precedence value, or to set a QoS group value for classification at the egress.

You can configure each marking action by using explicit values, table maps, or a combination of both. Table maps list specific traffic attributes and map (or convert) them to other attributes.

You can configure multiple conform, exceed, and violate actions simultaneously for each service class. If you do not configure a **violate-action**, by default the violate class is assigned the same action as the **exceed-action**.

After you create a table map, you configure a policy-map policer to use the table map.

Note When you use a table map in an input policy map, the protocol type for the **from**–action in the table map must be the same as the protocol type of the associated classification. For example, if a class map represents IP classification, the **from**–type action in the table map must be either **dscp** or **precedence**. If the class map represents a non-IP classification, the **from**–type action in the table map must be **cos**.

To configure multiple actions in a class, you can enter multiple conform, exceed, or violate action entries in policy-map class police configuration mode, as in this example:

```
Switch(config)# policy-map map1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police 100000 500000
Switch(config-pmap-c-police)# conform-action set-cos-transmit 4
Switch(config-pmap-c-police)# conform-action set-dscp-transmit dscp table
conform-dscp-to-dscp-mutation
Switch(config-pmap-c-police)# conform-action set-qos-transmit 10
Switch(config-pmap-c-police)# exceed-action set-cos-transmit 2
```

```
Switch(config-pmap-c-police)# exceed-action set-dscp-transmit dscp table
exceed-dscp-to-dscp-mutation
Switch(config-pmap-c-police)# exceed-action set-qos-transmit 20
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

Aggregate Policing

Aggregate policing applies only to input policy maps. An aggregate policer differs from an individual policer because it is shared by multiple traffic classes within a policy map. The switch module supports 1-rate, 2-color ingress policing and 2-rate, 3-color policing for aggregate policing.

You can use the **policer aggregate** global configuration command to set a policer for all traffic received or sent on a physical interface. When you configure an aggregate policer, you can configure specific burst sizes and conform and exceed actions. If you do not specify burst size (**bc**), the system calculates an appropriate burst size value. The calculated value is appropriate for most applications.

When you configure a 2-rate policer, in addition to configuring the committed information rate (CIR) for updating the first token bucket, you also configure the peak information rate (PIR) at which the second token bucket is updated. If you do not configure a PIR, the policer is a standard 1-rate, 2-color policer.

For 2-rate, 3-color policing, you can then optionally set actions to perform on packets that conform to the specified CIR and PIR (conform-action), packets that conform to the PIR, but not the CIR (exceed-action), and packets that exceed the PIR value (violate-action).

Note If the conform action is set to drop, the exceed and violate actions are automatically set to drop. If the exceed action is set to drop, the violate action is automatically set to drop.

- If you set the CIR value equal to the PIR, a traffic rate that is less than or equal to the CIR is in the conform range. Traffic that exceeds the CIR is in the violate range.
- If you set the PIR greater than the CIR, a traffic rate less than the CIR is in the conform range. A traffic rate that exceeds the CIR but is less than or equal to the PIR is in the exceed range. A traffic rate that exceeds the PIR is in the violate range.
- If you do not configure PIR, the policer is configured as a 1-rate, 2-color policer.

Setting the burst sizes too low can result in less traffic than expected. Setting burst sizes too high can result in more traffic than expected.

You can configure multiple conform and exceed actions simultaneously for each service class. Conform actions are to send the packet without modifications, to set a QoS group value for classification at the egress, or to set a new CoS, DSCP, or IP precedence value. Exceed actions are to drop the packet, to send the packet without modification, to set a QoS group for classification at the egress, or to set a new CoS, DSCP, or IP precedence to a value. You can configure each marking conform or exceed action by using explicit values, using table maps, or using a combination of both. Table maps list specific traffic attributes and map (or convert) them to other attributes.

You can configure multiple conform, exceed, and violate actions simultaneously for each service class. You can use the **conform-action**, **exceed-action**, and **violate-action** policy-map class configuration commands or the **conform-action**, **exceed-action**, and **violate-action** policy-map class police configuration commands to specify the action to be taken when the packet conforms to or exceeds the

specified traffic rates. Conform, exceed, and violate actions are to drop the packet, to send the packet without modifications, to set a new CoS, DSCP, or IP precedence value, or to set a QoS group value for classification at the egress.

Note If the conform action is set to drop, the exceed and violate actions are automatically set to drop. If the exceed action is set to drop, the violate action is automatically set to drop.

You can configure each marking conform, exceed, or violate action by using explicit values, using table maps, or using a combination of both. If you do not configure a **violate-action**, by default the violate class is assigned the same action as the **exceed-action**.

Table maps list specific traffic attributes and map (or convert) them to other attributes. Table maps are not supported for violate-action for aggregate policing unless you configure a table map for exceed-action and no explicit action is configured for violate action.

After you create a table map, you configure a policy-map policer to use the table map.

Note When you use a table map in an input policy map, the protocol type for the **from**–action in the table map must be the same as the protocol type of the associated classification. For example, if a class map represents IP classification, the **from**–type action in the table map must be either **dscp** or **precedence**. If the class map represents a non-IP classification, the **from**–type action in the table map must be **cos**.

You can configure multiple conform, exceed, and violate actions simultaneously for an aggregate policer as parameters in the **policer aggregate** global configuration command, but you must enter the actions in a particular order. See the configuration guideline in the "Configuring Input Policy Maps with Aggregate Policing" section on page 14-54.

After you configure the aggregate policer, you create a policy map and an associated class map, associate the policy map with the aggregate policer, and apply the service policy to a port.

Note Only one policy map can use any specific aggregate policer. Aggregate policing cannot be used to aggregate traffic streams across multiple interfaces. It can be used only to aggregate traffic streams across multiple classes in a policy map attached to an interface and aggregate streams across VLANs on a port in a per-port, per-VLAN policy map.

After you configure the policy map and policing actions, attach the policy to an ingress port by using the **service-policy** interface configuration command.

The class maps in this example refer to access lists.

```
Switch(config)# policer aggregate agg1 cir 23000 bc 10000 conform-action set-dscp-transmit
46 exceed-action drop
Switch(config)# class-map testclass
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map videoclass
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
Switch(config)# policy-map testexample
Switch(config-pmap)# class testclass
Switch(config-pmap-c)# police aggregate agg1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video-class
Switch(config-pmap-c)# police aggregate agg1
Switch(config-pmap-c)# exit
```

```
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input testexample
Switch(config-if)# exit
```

For configuration information, see the "Configuring Input Policy Maps with Aggregate Policing" section on page 14-54.

If the switch module is running the metro IP access or metro access image, you can also use aggregate policing to regulate traffic streams across VLANs, as in this example:

You can also use aggregate policing to regulate traffic streams across VLANs, as in this example:

```
Switch(config)# policer aggregate agg1 cir 23000 bc 10000 conform-action set-dscp-transmit
af31 set-cos-transmit 3 exceed-action set-dscp-transmit af11 set-cos-transmit 1
Switch(config)# class-map video-provider-1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map video-provider-2
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
Switch(config)# class-map match-any customer1-provider-100
Switch(config-cmap)# match vlan 100
Switch(config-cmap)# exit
Switch(config)# class-map match-any customer1-provider-200
Switch(config-cmap)# match vlan 200
Switch(config-cmap)# exit
Switch(config)# policy-map child-policy-1
Switch(config-pmap)# class video-provider-1
Switch(config-pmap-c)# set dscp af41
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# police aggregate agg1
Switch(config-pmap-c)# exit
Switch(config)# policy-map child-policy-2
Switch(config-pmap)# class video-provider-2
Switch(config-pmap-c)# set dscp cs4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# police aggregate agg1
Switch(config-pmap-c)# exit
Switch(config)# policy-map customer-1-ingress
Switch(config-pmap)# class customer1-provider-100
Switch(config-pmap-c)# service-policy child-policy-1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class customer1-provider-200
Switch(config-pmap-c)# service-policy child-policy-2
Switch(config-pmap-c)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# service-policy input customer-1-ingress
Switch(config-pmap-c)# exit
```

Unconditional Priority Policing

Priority policing applies only to output policy maps. You can use the **priority** policy-map class configuration command in an output policy map to designate a low-latency path, or class-based priority queuing, for a specific traffic class. With strict priority queuing, the packets in the priority queue are scheduled and sent until the queue is empty, at the expense of other queues. Excessive use of high-priority queuing can create congestion for lower priority traffic.

To eliminate this congestion, you can use the priority with police feature (priority policing) to reduce the bandwidth used by the priority queue and allocate traffic rates on other queues. Priority with police is the only form of policing supported in output policy maps.

Note You can configure 1-rate, 2-color policers for output policy maps with priority. You cannot configure 2-rate, 3-color policers for output policies.

See also the "Configuring Output Policy Maps with Class-Based Priority Queuing" section on page 14-72.

Note You cannot configure a policer committed burst size for an unconditional priority policer. Any configured burst size is ignored.

This example shows how to use the **priority** with **police** commands to configure *out-class1* as the priority queue, with traffic going to the queue limited to 20,000,000 bps so that the priority queue never uses more than that. Traffic above that rate is dropped. This allows other traffic queues to receive some port bandwidth, in this case a minimum bandwidth guarantee of 500,000 and 200,000 kbps. The class **class-default** queue gets the remaining port bandwidth.0

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police 200000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth 500000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth 200000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit
```

Marking

You can use packet marking in input policy maps to set or modify the attributes for traffic belonging to a specific class. After network traffic is organized into classes, you use marking to identify certain traffic types for unique handling. For example, you can change the CoS value in a class or set IP DSCP or IP precedence values for a specific type of traffic. These new values are then used to determine how the traffic should be treated. You can also use marking to assign traffic to a QoS group within the switch module.

Traffic marking is typically performed on a specific traffic type at the ingress port. The marking action can cause the CoS, DSCP, or precedence bits to be rewritten or left unchanged, depending on the configuration. This can increase or decrease the priority of a packet in accordance with the policy used in the QoS domain so that other QoS functions can use the marking information to judge the relative and absolute importance of the packet. The marking function can use information from the policing function or directly from the classification function.

You can specify and mark traffic by using the **set** commands in a policy map for all supported QoS markings (CoS, IP DSCP, IP precedence, and QoS groups). A **set** command unconditionally *marks* the packets that match a specific class. You then attach the policy map to an interface as an input policy map.

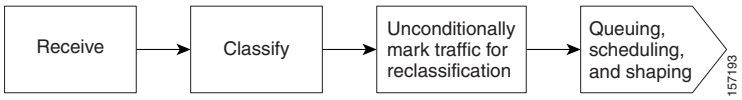
You can also mark traffic by using the **set** command with table maps.Table maps list specific traffic attributes and maps (or converts) them to another attribute. A table map establishes a to-from relationship for the attribute and defines the change to be made.

You can simultaneously configure actions to modify DSCP, precedence, and COS markings in the packet for the same service along with QoS group marking actions. You can use the QoS group number defined in the marking action for egress classification.

Note When you use a table map in an input policy map, the protocol type of the **from**-type action in the table map must be the same as the protocol type of the associated classification. For example, if a class map represents an IP classification, the **from**-type action in the table map must be either **dscp** or **precedence**. If the class map represents a non-IP classification, the **from**-type action in the table map must be **cos**.

After you create a table map, you configure a policy map to use the table map. See the "Congestion Management and Scheduling" section on page 14-26. Figure 14-6 shows the steps for marking traffic.

Figure 14-6 Marking of Classified Traffic



This example uses a policy map to remark a packet.

- The first marking (the **set** command) applies to the QoS default class map that matches all traffic not matched by class *AF31-AF33* and sets all traffic to an IP DSCP value of 1.
- The second marking sets the traffic in classes AF31 to AF33 to an IP DSCP of 3.

```
Switch(config)# policy-map Example
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set ip dscp 1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class AF31-AF33
Switch(config-pmap-c)# set ip dscp 3
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input Example
Switch(config-if)# exit
```

QoS Treatment for Performance-Monitoring Protocols

- Configuration Guidelines, page 14-25

Cisco IP-SLAs

For information about Cisco IP service level agreements (IP-SLAs), see "Understanding Cisco IOS IP SLAs."

QoS Treatment for IP-SLA and TWAMP Probes

The QoS treatment for IP-SLA and TWAMP probes must exactly reflect the effects that occur to the normal data traffic crossing the device.

The generating device should not change the probe markings. It should queue these probes based on the configured queueing policies for normal traffic.

Marking

By default, the class of service (CoS) marking of CFM traffic (including IP SLAs using CFM probes) is not changed. This feature cannot change this behavior.

By default, IP traffic marking (including IP SLA and TWAMP probes) is not changed. This feature can change this behavior.

Queuing

The CFM traffic (including IP SLAs using CFM probes) is queued according to its CoS value and the output policy map configured on the egress port, similar to normal traffic. This feature cannot change this behavior.

IP traffic (including IP SLA and TWAMP probes) is queued according to the markings specified in the **cpu traffic qos** global configuration command and the output policy map on the egress port. If this command is not configured, all IP traffic is statically mapped to a queue on the egress port.

QoS Marking for CPU-Generated Traffic

You can use QoS marking to set or modify the attributes of traffic from the CPU. The QoS marking action can cause the CoS, DSCP, or IP precedence bits in the packet to be rewritten or left unchanged. QoS uses packet markings to identify certain traffic types and how to treat them on the local switch module and the network.

You can also use marking to assign traffic to a QoS group within the switch module. This QoS group is an internal label that does not modify the packet, but it can be used to identify the traffic type when configuring egress queuing on the network port.

You can specify and mark traffic CPU-generated traffic by using these global configuration commands:

cpu traffic qos cos {*cos_value* | **cos** [**table-map** *table-map-name*] | **dscp** [**table-map** *table-map-name*] | **precedence** [**table-map** *table-map-name*]}

cpu traffic qos dscp {*dscp_value* | **cos** [**table-map** *table-map-name*] | **dscp** [**table-map** *table-map-name*] | **precedence** [**table-map** *table-map-name*]}

cpu traffic qos precedence {*precedence_value* | **cos** [**table-map** *table-map-name*] | **dscp** [**table-map** *table-map-name*] | **precedence** [**table-map** *table-map-name*]}

cpu traffic qos qos-group *value*

You can mark CoS, IP-DSCP, IP precedence, and QoS group by configuring an explicit value or by using the **table-map** keyword. Table maps list specific traffic attributes and map (or convert) them to another attribute. A table map establishes a to-from relationship for the attribute and defines the change to be made:

- Marking CoS by using the CoS, or the IP-DSCP, or the IP precedence of IP CPU-packets
- Marking CoS by using the CoS of non-IP CPU-packets.
- Marking IP DSCP by using the CoS, or the IP-DSCP, or the IP precedence of the CPU-packet
- Marking IP precedence by using the CoS, or the IP-DSCP, or the IP precedence of the CPU-packet

You can configure either IP-DSCP or IP precedence marking.

You can also simultaneously configure marking actions to modify CoS, IP-DSCP or IP precedence, and QoS group.

The **cpu traffic qos** command specifies the traffic to which it applies: all CPU traffic, only CPU IP traffic, or only CPU non-IP traffic. All other traffic retains its QoS markings. This feature does not affect CFM traffic (including Layer 2 IP SLA probes using CFM).

Note The switch module provides the ability to mark CoS, IP-DSCP and IP precedence of CPU-generated traffic by using table maps.

QoS Queuing for CPU-Generated Traffic

You can use the QoS markings established for the CPU-generated traffic by the **cpu traffic qos** global configuration command as packet identifiers in the class-map of an output policy-map to map CPU traffic to class-queues in the output policy-map on the egress port. You can then use output policy-maps on the egress port to configure queuing and scheduling for traffic leaving the switch module from that port.

If you want to map *all* CPU-generated traffic to a single class in the output policy-maps without changing the CoS, IP DSCP, or IP-precedence packet markings, you can use QoS groups for marking CPU-generated traffic.

If you want to map *all* CPU-generated IP traffic to classes in the output policy maps based on IP-DSCP or IP precedence without changing those packet markings, you can use a table map:

- Configure IP-DSCP or IP precedence marking by using **DSCP** or **precedence** as the **map from** value *without* a table map.
- Configure IP-DSCP or IP-precedence marking by using **DSCP** or **precedence** as the **map from** value *with* a table map, using only the **default** and **copy** keywords.

If you want to map *all* CPU-generated traffic to classes in the output policy maps based on the CoS without changing the CoS packet markings, you can use the table map:

- Configure CoS marking by using **CoS** as the **map from** value *without* a table map.
- Configure CoS marking using **CoS** as the **map from** value *with* a table map, using only the **default** and **copy** keywords.

For details about table maps, see the "Table Maps" section on page 14-14.

Using the **cpu traffic qos** global configuration command with table mapping, you can configure multiple marking and queuing policies to work together or independently. You can queue native VLAN traffic based on the CoS markings configured using the **cpu traffic qos** global configuration command.

The **cpu traffic qos** command specifies the traffic to which it applies: all CPU traffic, only CPU-IP traffic, or only CPU non-IP traffic. All other traffic is statically mapped to a CPU-default queue on the egress port. All CFM traffic (including Layer 2 IP SLA probes using CFM) is mapped to classes in the output policy map and queued based on their CoS value.

Note The switch module provides the ability to queue based on the CoS, IP-DSCP, and IP precedence of CPU-generated traffic.

Configuration Guidelines

- This feature must be configured globally for a switch module; it cannot be configured per-port or per-protocol.
- Enter each **cpu traffic qos** marking action on a separate line.
- The **cpu traffic qos cos** global configuration command configures CoS marking for CPU-generated traffic by using either a specific CoS value or a table map, but not both. A new configuration overwrites the existing configuration.
- The **cpu traffic qos dscp** global configuration command configures IP-DSCP marking for CPU-generated IP traffic by using either a specific DSCP value or a table map, but not both. A new configuration overwrites the existing configuration.
- The **cpu traffic qos precedence** global configuration command configures IP-precedence marking for CPU-generated IP traffic by using either a specific precedence value or a table map, but not both. A new configuration overwrites the existing configuration.
- The **cpu traffic qos dscp** and **cpu traffic qos precedence** global configuration commands are mutually exclusive. A new configuration overwrites the existing configuration.
- When the **cpu traffic qos dscp** global configuration command is configured with table maps, you can configure only one **map from** value at a time—DSCP, precedence, or CoS. A new configuration overwrites the existing configuration. Packets marked by this command can be classified and queued by an output policy map based on the marked DSCP or precedence value.
- When the **cpu traffic qos precedence** global configuration command is configured with table maps, you can configure only one **map from** value at a time—DSCP, precedence, or CoS. A new configuration overwrites the existing configuration. Packets marked by this command can be classified and queued by an output policy map based on the marked precedence or DSCP value.
- You cannot configure a **map from** value of both DSCP and precedence. A new configuration overwrites the existing configuration.
- When the **cpu traffic qos cos** global configuration command is configured with table maps, you can configure two **map from** values at a time—CoS and either DSCP or precedence.
- If the **cpu traffic qos cos** global configuration command is configured with only a **map from** value of DSCP or precedence:
  - The CoS value of IP packets is mapped by using the DSCP (or precedence) value in the packet and the configured table map. Packets can be classified and queued by an output policy map based on the marked CoS value.
  - The CoS value of non-IP packets remains unchanged.

- If the **cpu traffic qos cos** global configuration command is configured with a **map from** value of CoS:
  - The CoS value of IP packets is mapped by using the CoS value in the packet and the configured table map. Packets can be classified and queued by an output policy map based on the marked CoS value.
  - The CoS value of non-IP packets is mapped by using the CoS value in the packet and the configured table map. Packets can be classified and queued by an output policy map based on the marked CoS value.
- If the **cpu traffic qos cos** global configuration command is configured with a **map from** value of DSCP or precedence and CoS:
  - The CoS value of IP packets is mapped by using the DSCP or precedence value in the packet and the configured table map. Packets can be classified and queued by an output policy map based on the marked CoS value.
  - The CoS value of non-IP packets is mapped by using the CoS value in the packet and the configured table map. Packets can be classified and queued by an output policy map based on the marked CoS value.
- The **cpu traffic qos qos-group** global configuration command can be used to configure QoS group marking for CPU-generated traffic only for a specific QoS group. The **table-map** option is not available.

Congestion Management and Scheduling

Cisco Modular QoS CLI (MQC) provides several related mechanisms to control outgoing traffic flow. They are implemented in output policy maps to control output traffic queues. The scheduling stage holds packets until the appropriate time to send them to one of the four traffic queues. Queuing assigns a packet to a particular queue based on the packet class, and is enhanced by the WTD algorithm for congestion avoidance. You can use different scheduling mechanisms to provide a guaranteed bandwidth to a particular class of traffic while also serving other traffic in a fair way. You can limit the maximum bandwidth that can be consumed by a particular class of traffic and ensure that delay-sensitive traffic in a low-latency queue is sent before traffic in other queues.

The switch module supports these scheduling mechanisms:

- Traffic shaping

  You use the **shape average** policy map class configuration command to specify that a class of traffic should have a maximum permitted average rate. You specify the maximum rate in bits per second.

- Class-based-weighted-fair-queuing (CBWFQ)

  You can use the **bandwidth** policy-map class configuration command to control the bandwidth allocated to a specific class. Minimum bandwidth can be specified as a bit rate or a percentage of total bandwidth or of remaining bandwidth.

- Priority queuing or class-based priority queuing

  You use the **priority** policy-map class configuration command to specify the priority of a type of traffic over other types of traffic. You can specify strict priority for the high-priority traffic and allocate any excess bandwidth to other traffic queues, or specify priority with unconditional policing of high-priority traffic and allocate the known remaining bandwidth among the other traffic queues.

- To configure strict priority, use only the **priority** policy-map class configuration command to configure the priority queue. Use the **bandwidth remaining percent** policy-map class configuration command for the other traffic classes to allocate the excess bandwidth in the desired ratios.
- To configure priority with unconditional policing, configure the priority queue by using the **priority** policy-map class configuration command and the **police** policy-map class configuration command to unconditionally rate-limit the priority queue. In this case, you can configure the other traffic classes with **bandwidth** or **shape average**, depending on requirements.

These sections contain additional information about scheduling:

- Traffic Shaping, page 14-27
- Class-Based Weighted Fair Queuing, page 14-29
- Priority Queuing, page 14-30

Traffic Shaping

Traffic shaping is a traffic-control mechanism similar to traffic policing. While traffic policing is used in input policy maps, traffic shaping occurs as traffic leaves an interface. The switch module can apply class-based shaping to classes of traffic leaving an interface and port shaping to all traffic leaving an interface. Configuring a queue for traffic shaping sets the maximum bandwidth or peak information rate (PIR) of the queue.

Note You cannot configure traffic shaping (**shape average**) and CBWFQ (**bandwidth**) or priority queuing (**priority**) for the same class in an output policy map. You cannot configure traffic shaping for a traffic class when strict priority (priority without police) is configured for another class within the output policy-map.

Class-Based Shaping

Class-based shaping uses the **shape average** policy-map class configuration command to limit the rate of data transmission as the number of bits per second to be used for the committed information rate for a class of traffic. The switch module supports separate queues for three classes of traffic. The fourth queue is always the default queue for class **class-default**, unclassified traffic.

Note On the switch module, configuring traffic shaping also automatically sets the minimum bandwidth guarantee or committed information rate (CIR) of the queue to the same value as the PIR.

This example shows how to configure traffic shaping for outgoing traffic on a Fast Ethernet port so that *outclass1*, *outclass2*, and *outclass3* get a maximum of 50, 20, and 10 Mbps, respectively, of the available port bandwidth. The class **class-default** at a minimum gets the remaining bandwidth:

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class classout1
Switch(config-pmap-c)# shape average 50000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class classout2
Switch(config-pmap-c)# shape average 20000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class classout3
Switch(config-pmap-c)# shape average 10000000
```

```
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

Port Shaping

To configure port shaping (a transmit port shaper), create a policy map that contains only a default class, and use the **shape average** command to specify the maximum bandwidth for a port.

This example shows how to configure a policy map that shapes a port to 90 Mbps, allocated according to the *out-policy* policy map configured in the previous example. The **service-policy** policy map class command is used to create a child policy to the parent:

```
Switch(config)# policy-map out-policy-parent
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 90000000
Switch(config-pmap-c)# service-policy out-policy
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output out-policy-parent
Switch(config-if)# exit
```

Parent-Child Hierarchy

The switch module also supports *parent* policy levels and *child* policy levels for traffic shaping. The QoS parent-child structure is used for specific purposes where a child policy is referenced in a parent policy to provide additional control of a specific traffic type.

The first policy level, the parent level, is used for port shaping, and you can specific only one class of type **class-default** within the policy. This is an example of a parent-level policy map:

```
Switch(config)# policy-map parent
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 50000000
Switch(config-pmap-c)# exit
```

The second policy level, the *child* level, is used to control a specific traffic stream or class, as in this example:

```
Switch(config)# policy-map child
Switch(config-pmap)# class class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
```

Note The total of the minimum bandwidth guarantees (CIR) for each queue of the child policy cannot exceed the total port-shape rate.

This is an example of a parent-child configuration:

```
Switch(config)# policy-map parent
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 50000000
Switch(config-pmap-c)# service-policy child
Switch(config-pmap-c)# exit
```

```
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output parent
Switch(config-if)# exit
```

Class-Based Weighted Fair Queuing

You can configure class-based weighted fair queuing (CBWFQ) to set the relative precedence of a queue by allocating a portion of the total bandwidth that is available for the port. You use the **bandwidth** policy-map class configuration command to set the output bandwidth for a class of traffic as a rate (kilobits per second), a percentage of total bandwidth, or a percentage of remaining bandwidth.

Note When you configure bandwidth in a policy map, you must configure all rates in the same format, either a configured rate or a percentage. The total of the minimum bandwidth guarantees (CIR) for each queue of the policy cannot exceed the total speed of the parent.

- When you use the **bandwidth** policy-map class configuration command to configure a class of traffic as an absolute rate (kilobits per second) or a percentage of total bandwidth, this represents the minimum bandwidth guarantee (CIR) for that traffic class. This means that the traffic class gets at least the bandwidth indicated by the command, but is not limited to that bandwidth. Any excess bandwidth on the port is allocated to each class in the same ratio in which the CIR rates are configured.

  Note You cannot configure bandwidth as an absolute rate or a percentage of total bandwidth when strict priority (priority without police) is configured for another class in the output policy.

- When you use the **bandwidth** policy-map class configuration command to configure a class of traffic as a percentage of *remaining* bandwidth, this represents the portion of the excess bandwidth of the port that is allocated to the class. This means that the class is allocated bandwidth only if there is excess bandwidth on the port, and if there is no minimum bandwidth guarantee for this traffic class.

  Note You can configure bandwidth as percentage of remaining bandwidth only when strict priority (priority without police) is configured for another class in the output policy map.

For more information, see the "Configuring Output Policy Maps with Class-Based-Weighted-Queuing" section on page 14-67.

Note You cannot configure bandwidth and traffic shaping (**shape average**) or priority queuing (**priority**) for the same class in an output policy map.

This example shows how to set the precedence of output queues by setting bandwidth in kilobits per second. The classes *outclass1*, *outclass2*, and *outclass3* and **class-default** get a minimum of 40000, 20000, 10000, and 10000 kbps. Any excess bandwidth is divided among the classes in the same proportion as the CIR rated:

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth 40000
```

```
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth 20000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth 10000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth 10000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

Note When you configure CIR bandwidth for a class as an absolute rate or percentage of the total bandwidth, any excess bandwidth remaining after servicing the CIR of all the classes in the policy map is divided among the classes in the same proportion as the CIR rates. If the CIR rate of a class is configured as 0, that class is also not eligible for any excess bandwidth and as a result receives no bandwidth.

This example shows how to allocate the excess bandwidth among queues by configuring bandwidth for a traffic class as a percentage of remaining bandwidth. The class *outclass1* is given priority queue treatment. The other classes are configured to get percentages of the excess bandwidth if any remains after servicing the priority queue: *outclass2* is configured to get 50 percent, *outclass3* to get 20 percent, and the class **class-default** to get the remaining 30 percent.

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

Priority Queuing

You can use the **priority** policy-map class configuration command to ensure that a particular class of traffic is given preferential treatment. With strict priority queuing, the priority queue is constantly serviced. All packets in the queue are scheduled and sent until the queue is empty. Priority queuing allows traffic for the associated class to be sent before packets in other queues are sent.

Note You should exercise care when using the **priority** command. Excessive use of strict priority queuing might cause congestion in other queues.

The switch module supports strict priority queuing or priority used with the **police** policy-map command.

- *Strict priority queuing* (priority without police) assigns a traffic class to a low-latency queue to ensure that packets in this class have the lowest possible latency. When this is configured, the priority queue is continually serviced until it is empty, possibly at the expense of packets in other queues.

Note You cannot configure priority without policing for a traffic class when traffic shaping or CBWFQ are configured for another class in the same output policy map.

- You can use priority with the **police** policy-map command, or *unconditional priority policing*, to reduce the bandwidth used by the priority queue. This is the only form of policing that is supported in output policy maps. Using this combination of commands configures a maximum rate on the priority queue, and you can use the **bandwidth** and **shape average** policy-map commands for other classes to allocate traffic rates on other queues.

Note When priority is configured in an output policy map *without* the **police** command, you can only configure the other queues for sharing by using the **bandwidth remaining percent** policy-map command to allocate excess bandwidth.

Priority queuing has these restrictions:

- You can associate the **priority** command with a single unique class for all attached output polices on the switch module.
- You cannot configure priority and any other scheduling action (**shape average** or **bandwidth**) in the same class.
- You cannot configure priority queuing for the **class-default** of an output policy map.

For more information, see the "Configuring Output Policy Maps with Class-Based Priority Queuing" section on page 14-72.

This example shows how to configure the class *out-class1* as a strict priority queue so that all packets in that class are sent before any other class of traffic. Other traffic queues are configured so that *out-class-2* gets 50 percent of the remaining bandwidth and *out-class3* gets 20 percent of the remaining bandwidth. The class **class-default** receives the remaining 30 percent with no guarantees.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit
```

This example shows how to use the **priority** with **police** commands to configure *out-class1* as the priority queue, with traffic going to the queue limited to 20000000 bps so that the priority queue will never use more than that. Traffic above that rate is dropped. The other traffic queues are configured to use 50 and 20 percent of the bandwidth that is left, as in the previous example.

```
Switch(config)# policy-map policy1
```

```
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police 200000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit

Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit
```

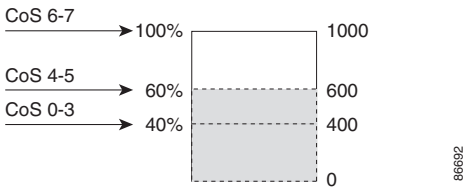
Congestion Avoidance and Queuing

Congestion avoidance uses algorithms such as tail drop to control the number of packets entering the queuing and scheduling stage to avoid congestion and network bottlenecks. The switch module uses Weighted Tail Drop (WTD) to manage the queue sizes and provide a drop precedence for traffic classifications. You set the queue size limits depending on the markings of the packets in the queue. Each packet that travels through the switch module can be assigned to a specific queue and threshold. For example, specific DSCP or CoS values can be mapped to a specific egress queue and threshold.

WTD is implemented on traffic queues to manage the queue size and to provide drop precedences for different traffic classifications. As a frame enters a particular queue, WTD uses the packet classification to subject it to different thresholds. If the total destination queue size is greater than the threshold of any reclassified traffic, the next frame of that traffic is dropped.

Figure 14-7 shows an example of WTD operating on a queue of 1000 frames. Three drop percentages are configured: 40 percent (400 frames), 60 percent (600 frames), and 100 percent (1000 frames). These percentages mean that traffic reclassified to the 40-percent threshold is dropped when the queue depth exceeds 400 frames, traffic reclassified to 60 percent is dropped when the queue depth exceeds 600 frames, and traffic up to 400 frames can be queued at the 40-percent threshold, up to 600 frames at the 60-percent threshold, and up to 1000 frames at the 100-percent threshold.

Figure 14-7 WTD and Queue Operation



In this example, CoS values 6 and 7 have a greater importance than the other CoS values, and they are assigned to the 100-percent drop threshold (queue-full state). CoS values 4 and 5 are assigned to the 60-percent threshold, and CoS values 0 to 3 are assigned to the 40-percent threshold.

If the queue is already filled with 600 frames, and a new frame arrives containing CoS values 4 and 5, the frame is subjected to the 60-percent threshold. When this frame is added to the queue, the threshold would be exceeded, so the switch module drops it.

WTD is configured by using the **queue-limit** policy-map class command. The command adjusts the queue size (buffer size) associated with a particular class of traffic. You specify the threshold as the number of packets, where each packet is a fixed unit of 256 bytes. You can specify different queue sizes for different classes of traffic (CoS, DSCP, precedence, or QoS group) in the same queue. Setting a queue limit establishes a drop threshold for the associated traffic when congestion occurs.

Note You cannot configure queue size by using the **queue-limit** policy map class command without first configuring a scheduling action (**bandwidth**, **shape average**, or **priority**). The only exception to this is when you configure queue-limit for the **class-default** of an output policy map.

The switch module supports up to three unique queue-limit configurations across all output policy maps. Within an output policy map, only four queues (classes) are allowed, including the class default. Each queue has three thresholds defined. Only three unique threshold value configurations are allowed on the switch module. However, multiple policy maps can share the same queue-limits. When two policy maps a share queue-limit configuration, all threshold values must be the same for all the classes in both policy maps.

For more information, see the "Configuring Output Policy Maps with Class-Based-Weighted-Queuing" section on page 14-67.

This example configures *class A* to match DSCP values and a policy map, *PM1*. The DSCP values of 30 and 50 are mapped to unique thresholds (32 and 64, respectively). The DSCP values of 40 and 60 are mapped to the maximum threshold of 112 packets.

```
Switch(config)# class-map match-any classA
Switch(config-cmap)# match ip dscp 30 40 50 60
Switch(config-cmap)# exit
Switch(config)# policy-map PM1
Switch(config-pmap)# class classA
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# queue-limit 112
Switch(config-pmap-c)# queue-limit dscp 30 32
Switch(config-pmap-c)# queue-limit dscp 50 64
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# service-policy output PM1
Switch(config-if)# exit
```

You can use these same queue-limit values in multiple output policy maps on the switch module. However, changing one of the queue-limit values in a class creates a new, unique queue-limit configuration. You can attach only three unique queue-limit configurations in output policy maps to interfaces at any one time. If you attempt to attach an output policy map with a fourth unique queue-limit configuration, you see this error message:

```
QoS: Configuration failed. Maximum number of allowable unique queue-limit
configurations exceeded.
```

Note When you configure a queue limit for a class in an output policy map, all other output policy maps must use the same qualifier type and qualifier value format. Only the queue-limit threshold values can be different. For example, when you configure *class A* queue limit thresholds for **dscp 30** and **dscp 50** in policy map *PM1*, and you configure *class A* queue limits in policy map *PM2*, you must use **dscp 30** and **dscp 50** as qualifiers. You cannot use **dscp 20** and **dscp 40**. The threshold values can be different, but different threshold values creates a new queue-limit configuration.

By default, the total amount of buffer space is divided equally among all ports and all queues per port, which is adequate for many applications. You can decrease the queue size for latency-sensitive traffic or increase the queue size for bursty traffic.

Note When you use the **queue-limit** command to configure queue thresholds for a class, the WTD thresholds must be less than or equal to the queue maximum threshold. A queue size configured with no qualifier must be larger than any queue sizes configured with qualifiers.

When you configure queue limit, the range for the number of packets is from 16 to 544, in multiples of 16, where each packet is a fixed unit of 256 bytes.

Note For optimal performance, we strongly recommend that you configure the queue-limit to 272 or less.

Queue bandwidth and queue size (queue limit) are configured separately and are not interdependent. You should consider the type of traffic being sent when you configure bandwidth and queue-limit:

- A large buffer (queue limit) can better accommodate bursty traffic without packet loss, but at the cost of increased latency.
- A small buffer reduces latency but is more appropriate for steady traffic flows than for bursty traffic.
- Very small buffers are typically used to optimize priority queuing. For traffic that is priority queued, the buffer size usually needs to accommodate only a few packets; large buffer sizes that increase latency are not usually necessary. For high-priority latency-sensitive packets, configure a relatively large bandwidth and relatively small queue size.

Note These restrictions apply to WTD qualifiers:

- You cannot configure more than two threshold values for WTD qualifiers (**cos**, **dscp**, **precedence**, **qos-group**) by using the **queue-limit** command. However, there is no limit to the number of qualifiers that you can map to these thresholds. You can configure a third threshold value to set the maximum queue by using the **queue-limit** command with no qualifiers.
- A WTD qualifier in the **queue-limit** command must be the same as at least one **match** qualifier in the associated class map.

This example shows how to configure bandwidth and queue limit so that *out-class1*, *out-class2*, *out-class3*, and **class-default** get a minimum of 40, 20, 10 and 10 percent of the traffic bandwidth, respectively. The corresponding queue-sizes are set to 48, 32, 16 and 272 (256-byte) packets:

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth percent 40
Switch(config-pmap-c)# queue-limit 48
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# queue-limit 32
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 16
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
```

```
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 272
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

You can configure and attach as many output policy maps as there are switch module ports, but only three unique queue-limit configurations are allowed. When another output policy map uses the same queue-limit and class configurations, even if the bandwidth percentages are different, it is considered to be the same queue-limit configuration.

Configuring QoS

Before configuring QoS, you must have a thorough understanding of these factors:

- The types of applications used and the traffic patterns on your network.
- Traffic characteristics and needs of your network. Is the traffic bursty? Do you need to reserve bandwidth for voice and video streams?
- Bandwidth requirements and speed of the network.
- Location of congestion points in the network.

These sections describe how to classify, police, and mark incoming traffic, and schedule and queue outgoing traffic. Depending on your network configuration, you must perform one or more of these tasks.

- Default QoS Configuration, page 14-35
- QoS Configuration Guidelines, page 14-36
- Using ACLs to Classify Traffic, page 14-37
- Using Class Maps to Define a Traffic Class, page 14-42
- Configuring Table Maps, page 14-45
- Attaching a Traffic Policy to an Interface, page 14-47
- Configuring Input Policy Maps, page 14-47
- Configuring Output Policy Maps, page 14-66
- Configuring QoS Marking and Queuing for CPU-Generated Traffic, page 14-80

Default QoS Configuration

There are no policy maps, class maps, table maps, or policers configured. At the egress port, all traffic goes through a single default queue that is given the full operational port bandwidth. The default size of the default queue is 160 (256-byte) packets.

The packets are not modified (the CoS, DSCP, and IP precedence values in the packet are not changed). Traffic is switched in pass-through mode without any rewrites and classified as best effort without any policing.

QoS Configuration Guidelines

- You can configure QoS only on physical ports.
- On a port configured for QoS, all traffic received through the port is classified, policed, and marked according to the input policy map attached to the port. On a trunk port configured for QoS, traffic in all VLANs received through the port is classified, policed, and marked according to the policy map attached to the port. If a per-port, per-VLAN policy map is attached, traffic on the trunk port is classified, policed, and marked for the VLANs specified in the parent-level policy, according to the child policy map associated with each VLAN.
- If you have EtherChannel ports configured on your switch module, you must configure QoS classification, policing, mapping, and queuing on the individual physical ports that comprise the EtherChannel. You must decide whether the QoS configuration should match on all ports in the EtherChannel.
- Control traffic (such as spanning-tree bridge protocol data units [BPDUs] and routing update packets) received by the switch module are subject to all ingress QoS processing.
- You are likely to lose data when you change queue settings; try to make changes when traffic is at a minimum.
- When you try to attach a new policy to an interface and this brings the number of policer *instances* to more than 1,024 minus 1 more than the number of interfaces on the switch module, you receive an error message, and the configuration fails.
- When you try to attach new policy to an interface, increasing the number of policer profiles to more than 256, you receive an error message, and the configuration fails. A profile is a combination of commit rate, peak rate, commit burst, and peak burst. You can attach one profile to multiple instances, but if one of these characteristics differs, the policer is considered to have a new profile.
- You can specify 256 *unique* VLAN classification criteria within a per-port, per-VLAN policy-map, across all ports on the switch module. Any policy attachment or change that causes this limit to be exceeded fails with a *VLAN label resources exceeded* error message.
- You can attach per-port and per-port, per-VLAN policy-maps across all ports on the switch module until QoS ACE classification resource limitations are reached. Any policy attachment or change that causes this limit to be exceeded fails with a *TCAM resources exceeded* error message.
- When CPU protection is enabled, you can configure only 45 policers per port. Disabling CPU protection allows you to configure up to 64 policers per port. You can enter the **show policer cpu uni-eni** {**drop** | **rate**} privileged EXEC command to see if CPU protection is enabled.
- Note these limitations when you disable CPU protection:
  - When CPU protection is disabled, you can configure a maximum of 63 policers per port for user-defined classes, and one for class-default. Any policy attachment or change that causes this limit to be exceeded fails with a *policer resources exceeded* error message.
  - When CPU protection is disabled, you can configure a maximum of 256 policers on the switch modulefor ME3400-24TS ME3400E-24TS platform. Any policy attachment or change that causes this limit to be exceeded fails with a *policer resources exceeded* error message.
  - If you disable CPU protection and attach a policy map with more than 45 policers, and then enable CPU protection again, and reload, 19 policers per port are again required for CPU protection. During reload, the policers 46 and above will reach the *policer resources exceeded* error condition and no policers are attached to those classes.
- If the number of internal QoS labels exceeds 256, you receive an error message.

- Table maps are not supported for **violate-action** for aggregate policing unless you configure a table map for exceed-action and no explicit action is configured for **violate-action**. For both individual and aggregate policers, if you do not configure a **violate-action**, by default the violate class is assigned the same action as the **exceed-action**.
- If double-tagged packets are received on a trunk or 802.1Q tunnel interface, these packets can be classified on DSCP and IP precedence along with other parameters, but you cannot set DSCP or IP precedence on the outgoing packets. You can set CoS on the outgoing packets.

See the configuration sections for specific QoS features for more configuration guidelines related to each feature.

Using ACLs to Classify Traffic

You can classify IP traffic by using IP standard or IP extended ACLs. You can classify IP and non-IP traffic by using Layer 2 MAC ACLs. For more information about configuring ACLs, see Chapter 34, “Configuring Network Security with ACLs" in the *Cisco CGS 2520 Switch Software Configuration Guide*:

http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swacl.html

Follow these guidelines when configuring QoS ACLs:

- You cannot match IP fragments against configured IP extended ACLs to enforce QoS. IP fragments are sent as best-effort. IP fragments are denoted by fields in the IP header.
- The switch module supports only one access group per class in an input policy map.
- You cannot configure **match-access** group in an output policy map.

These sections describe how to create QoS ACLs:

- “Creating IP Standard ACLs” section on page 14-38
- “Creating IP Extended ACLs” section on page 14-39
- “Creating Layer 2 MAC ACLs” section on page 14-40

Creating IP Standard ACLs

Beginning in privileged EXEC mode, follow these steps to create an IP standard ACL for IP traffic:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Create an IP standard ACL, repeating the command as many times as necessary. • For *access-list-number*, enter the access list number. The range is 1 to 99 and 1300 to 1999. • Always use the **permit** keyword for ACLs used as match criteria in QoS policies. QoS policies do not match ACLs that use the **deny** keyword. • For *source*, enter the network or host from which the packet is being sent. You can use the **any** keyword as an abbreviation for 0.0.0.0 255.255.255.255. • (Optional) For *source-wildcard*, enter the wildcard bits in dotted decimal notation to be applied to the source.	**access-list** *access-list-number* **permit** *source* [*source-wildcard*]
Step 3	Define a standard IPv4 access list using a name, and enter access-list configuration mode. The name can be a number from 1 to 99. In access-list configuration mode, enter **permit** *source* [*source-wildcard*]	**ip access-list standard** *name*
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entries.	**show access-lists**

To delete an access list, use the **no access-list** *access-list-number* global configuration command.

This example shows how to allow access for only those hosts on the three specified networks. The wildcard bits apply to the host portions of the network addresses:

```
Switch(config)# access-list 1 permit 192.5.255.0 0.0.0.255
Switch(config)# access-list 1 permit 128.88.0.0 0.0.255.255
Switch(config)# access-list 1 permit 36.0.0.0 0.0.0.255
```

Creating IP Extended ACLs

Beginning in privileged EXEC mode, follow these steps to create an IP extended ACL for IP traffic:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Create an IP extended ACL. Repeat the step as many times as necessary. • For *access-list-number*, enter the access list number. The range is 100 to 199 and 2000 to 2699. • Always use the **permit** keyword for ACLs used as match criteria in QoS policies. QoS policies do not match **deny** ACLs. • For *protocol*, enter the name or number of an IP protocol. Use the question mark (?) to see a list of available protocols. To match any Internet protocol (including ICMP, TCP, and UDP), enter **ip**. • The *source* is the number of the network or host sending the packet. • The *source-wildcard* applies wildcard bits to the source. • The *destination* is the network or host number receiving the packet. • The *destination-wildcard* applies wildcard bits to the destination. You can specify source, destination, and wildcards as: • The 32-bit quantity in dotted-decimal format. • The keyword **any** for 0.0.0.0 255.255.255.255 (any host). • The keyword **host** for a single host 0.0.0.0. Other keywords are optional and have these meanings: • **precedence**—Enter to match packets with a precedence level specified as a number from 0 to 7 or by name: **routine** (**0**), **priority** (**1**), **immediate** (**2**), **flash** (**3**), **flash-override** (**4**), **critical** (**5**), **internet** (**6**), **network** (**7**). • **tos**—Enter to match by type of service level, specified by a number from 0 to 15 or a name: **normal** (**0**), **max-reliability** (**2**), **max-throughput** (**4**), **min-delay** (**8**). • **dscp**—Enter to match packets with the DSCP value specified by a number from 0 to 63, or use the question mark (?) to see a list of available values.	**access-list** *access-list-number* **permit** *protocol* {*source source-wildcard destination destination-wildcard*} [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] **Note** If you enter a **dscp** value, you cannot enter **tos** or **precedence**. You can enter both a **tos** and a **precedence** value with no **dscp**.

	Step	Command
Step 3	Define an extended IPv4 access list using a name, and enter access-list configuration mode. The *name* can be a number from 100 to 199. In access-list configuration mode, enter **permit** *protocol* {*source source-wildcard destination destination-wildcard*} [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] as defined in Step 2.	**ip access-list extended** *name*
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entries.	**show access-lists**

To delete an access list, use the **no access-list** *access-list-number* global configuration command.

This example shows how to create an ACL that permits IP traffic from any source to any destination that has the DSCP value set to 32:

```
Switch(config)# access-list 100 permit ip any any dscp 32
```

This example shows how to create an ACL that permits IP traffic from a source host at 10.1.1.1 to a destination host at 10.1.1.2 with a precedence value of 5:

```
Switch(config)# access-list 100 permit ip host 10.1.1.1 host 10.1.1.2 precedence 5
```

Creating Layer 2 MAC ACLs

Beginning in privileged EXEC mode, follow these steps to create a Layer 2 MAC ACL for non-IP traffic:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Create a Layer 2 MAC ACL by specifying the name of the list and enter extended MAC ACL configuration mode.	**mac access-list extended** *name*

	Step	Command
Step 3	Always use the **permit** keyword for ACLs used as match criteria in QoS policies. • For *src-MAC-addr*, enter the MAC address of the host from which the packet is being sent. You can specify in hexadecimal format (H.H.H), use the **any** keyword for *source* 0.0.0, *source-wildcard* ffff.ffff.ffff, or use the **host** keyword for *source* 0.0.0. • For *mask,* enter the wildcard bits by placing ones in the bit positions that you want to ignore. • For *dst-MAC-addr*, enter the MAC address of the host to which the packet is being sent. You can specify in hexadecimal format (H.H.H), use the **any** keyword for *source* 0.0.0, *source-wildcard* ffff.ffff.ffff, or use the **host** keyword for *source* 0.0.0. • (Optional) For *type mask*, specify the Ethertype number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet. For *type*, the range is from 0 to 65535, typically specified in hexadecimal. For *mask*, enter the *don't care* bits applied to the Ethertype before testing for a match.	**permit** {**host** *src-MAC-addr mask* | **any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask*]
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entries.	**show access-lists** [*access-list-number* | *access-list-name*]
Step 6	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To delete an access list, use the **no mac access-list extended** *access-list-name* global configuration command.

This example shows how to create a Layer 2 MAC ACL with two **permit** statements. The first statement allows traffic from the host with MAC address 0001.0000.0001 to the host with MAC address 0002.0000.0001. The second statement allows only Ethertype XNS-IDP traffic from the host with MAC address 0001.0000.0002 to the host with MAC address 0002.0000.0002:

```
Switch(config)# mac access-list extended maclist1
Switch(config-ext-macl)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Switch(config-ext-macl)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
Switch(config-ext-macl)# exit
```

Using Class Maps to Define a Traffic Class

You use the **class-map** global configuration command to name and to isolate a specific traffic flow (or class) from all other traffic. A class map defines the criteria to use to match against a specific traffic flow to further classify it. Match statements can include criteria such as an ACL, CoS value, DSCP value, IP precedence values, QoS group values, or VLAN IDs. You define match criterion with one or more **match** statements entered in the class-map configuration mode.

Follow these guidelines when configuring class maps:

- A **match-all** class map cannot have more than one classification criterion (one match statement), but a **match-any** class map can contain multiple match statements.
- The **match cos** and **match vlan** commands are supported only on Layer 2 802.1Q trunk ports.
- You use a class map with the **match vlan** command in the parent policy in input hierarchical policy maps for per-port, per-VLAN QoS on trunk ports. A policy is considered a parent policy map when it has one or more of its classes associated with a child policy map. Each class within a parent policy map is called a parent class. You can configure only the **match vlan** command in parent classes. You cannot configure the **match vlan** command in classes within the child policy map.
- For an input policy map, you cannot configure an IP classification (**match ip dscp**, **match ip precedence**, **match access-group** for an IP ACL) and a non-IP classification (**match cos** or **match access-group** for a MAC ACL) in the same policy map or class map. For a per-port, per-VLAN hierarchical policy map, this applies to the child policy map.
- You cannot configure **match qos-group** for an input policy map.
- In an output policy map, no two class maps can have the same classification criteria; that is, the same match qualifiers and values.
- The maximum number of class maps on the switch module is 1024.

Beginning in privileged EXEC mode, follow these steps to create a class map and to define the match criterion to classify traffic:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Create a class map, and enter class-map configuration mode. By default, no class maps are defined. • (Optional) Use the **match-all** keyword to perform a logical-AND of all matching statements under this class map. All match criteria in the class map must be matched. • (Optional) Use the **match-any** keyword to perform a logical-OR of all matching statements under this class map. One or more match criteria must be matched. • For *class-map-name*, specify the name of the class map. If no matching statements are specified, the default is **match-all**. **Note** A **match-all** class map cannot have more than one classification criterion (match statement).	**class-map** [**match-all** | **match-any**] *class-map-name*

	Step	Command
Step 3	Define the match criterion to classify traffic. By default, no match criterion is defined. Only one match type per class map is supported, and only one ACL per class map is supported. • For **access-group** *acl-index-or-name,* specify the number or name of an ACL. Matching access groups is supported only in input policy maps. • For **cos** *cos-list*, enter a list of up to four CoS values in a single line to match against incoming packets. Separate each value with a space. You can enter multiple *cos-list* lines to match more than four CoS values. The range is 0 to 7. • For **ip dscp** *dscp-list*, enter a list of up to eight IPv4 DSCP values to match against incoming packets. Separate each value with a space. You can enter multiple *dscp-list* lines to match more than eight DSCP values. The numerical range is 0 to 63. You can also configure DSCP values in other forms. See the "Classification Based on IP DSCP" section on page 14-8. • For **ip precedence** *ip-precedence-list*, enter a list of up to four IPv4 precedence values to match against incoming packets. Separate each value with a space. You can enter multiple *ip-precedence-list* lines to match more than four precedence values. The range is 0 to 7. • For **vlan** *vlan-list,* specify a VLAN ID or a range of VLANs to be used in a parent policy map for per-port, per-VLAN QoS on a trunk port. The VLAN ID range is 1 to 4094. • For **qos-group** *value,* specify the QoS group number. The range is 0 to 99. Matching of QoS groups is supported only in output policy maps.	**match** {**access-group** *acl-index-or-name* | **cos** *cos-list* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list* | **qos-group** *value* | **vlan** *vlan-list*}
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entries.	**show class-map**
Step 6	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

Use the **no** form of the appropriate command to delete an existing class map or remove a match criterion.

This example shows how to create access list 103 and configure the class map called *class1*. The *class1* has one match criterion, which is access list 103. It permits traffic from any host to any destination that matches a DSCP value of 10.

```
Switch(config)# access-list 103 permit any any dscp 10
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# exit
```

This example shows how to create a class map called *class2*, which matches incoming traffic with DSCP values of 10, 11, and 12:

```
Switch(config)# class-map match-any class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# exit
```

This example shows how to create a class map called *class3*, which matches incoming traffic with IP-precedence values of 5, 6, and 7:

```
Switch(config)# class-map match-any class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# exit
```

This example shows how to create a parent class-map called *parent-class*, which matches incoming traffic with VLAN IDs in the range from 30 to 40:

```
Switch(config)# class-map match-any parent-class
Switch(config-cmap)# match vlan 30-40
Switch(config-cmap)# exit
```

Configuring Table Maps

You can configure table maps to manage a large number of traffic flows with a single command. You use table maps to correlate specific DSCP, IP precedence and CoS values to each other, to mark down a DSCP, IP precedence, or CoS value, or to assign default values. You can specify table maps in **set** commands and use them as mark-down mapping for the policers.

These table maps are supported on the switch module:

- DSCP to CoS, precedence, or DSCP
- CoS to DSCP, precedence, or CoS
- Precedence to CoS, DSCP, or precedence

Note these guidelines when configuring table maps:

- The switch module supports a maximum of 256 unique table maps.
- The maximum number of map statements within a table map is 64.
- Table maps cannot be used in output policy maps.
- Table maps are not supported for **violate-action** for aggregate policing unless you configure a table map for **exceed-action** and no explicit action is configured for **violate-action**.

Beginning in privileged EXEC mode, follow these steps to create a table map:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Create a table map by entering a table-map name and entering table-map configuration mode.	**table-map** *table-map-name*
Step 3	Enter the mapping values to be included in the table. For example, if the table map is a DSCP-to-CoS table map, the *from-value* would be the DSCP value and the *to_value* would be the CoS value. Both ranges are from 0 to 63. Enter this command multiple times to include all the values that you want to map.	**map from** *from-value* **to** *to-value*
Step 4	Set the default behavior for a value not found in the table map. • Enter a *default-value* to specify a certain value. For example, in a DSCP-to-CoS table map, this would be a specific CoS value to apply to all unmapped DSCP values. The range is from 0 to 63. • Enter **copy** to map unmapped values to an equivalent value. In a DSCP-to-CoS table map, this command maps all unmapped DSCP values to the equivalent CoS value. • Enter **ignore** to leave unmapped values unchanged. In a DSCP-to-CoS table map, the switch module does not change the CoS value of unmapped DSCP values.	**default** {*default-value* | **copy** | **ignore**}
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify your entries.	**show table-map** [*table-map-name*]
Step 7	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To delete a table map, use the **no table-map** *table-map-name* global configuration command.

This example shows how to create a DSCP-to-CoS table map. A complete table would typically include additional map statements for the higher DSCP values. The default of 4 in this table means that unmapped DSCP values will be assigned a CoS value of 4:

```
Switch(config)# table-map dscp-to-cos
Switch(config-tablemap)# map from 1 to 1
Switch(config-tablemap)# map from 2 to 1
Switch(config-tablemap)# map from 3 to 1
Switch(config-tablemap)# map from 4 to 2
Switch(config-tablemap)# map from 5 to 2
Switch(config-tablemap)# map from 6 to 3
Switch(config-tablemap)# default 4
Switch(config-tablemap)# end
Switch# show table-map dscp-to-cos
```

Attaching a Traffic Policy to an Interface

You use the **service-policy** interface configuration command to attach a traffic policy to an interface and to specify the direction in which the policy should be applied: either an input policy map for incoming traffic or an output policy map for outgoing traffic. Input and output policy maps support different QoS features. See the "Configuring Input Policy Maps" section on page 14-47 and the "Configuring Output Policy Maps" section on page 14-66 for restrictions on input and output policy maps.

You can attach a service policy only to a physical port. You can attach only one input policy map and one output policy map per port.

Note If you enter the **no** policy-map configuration command or the **no policy-map** *policy-map-name* global configuration command to delete a policy map that is attached to an interface, a warning message appears that lists any interfaces from which the policy map is being detached. The policy map is then detached and deleted. For example:

```
Warning: Detaching Policy test1 from Interface GigabitEthernet0/1
```

Beginning in privileged EXEC mode, follow these steps to attach a policy map to a port:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the port to attach to the policy map, and enter interface configuration mode. Valid interfaces are physical ports.	**interface** *interface-id*
Step 3	Specify the policy-map name and whether it is an input policy map or an output policy map.	**service-policy** {**input** | **output**} *policy-map-name*
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entries.	**show policy-map interface** [*interface-id*]
Step 6	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To remove the policy map and port association, use the **no service-policy** {**input** | **output**} *policy-map-name* interface configuration command.

Configuring Input Policy Maps

Policy maps specify which traffic class to act on and what actions to take. All traffic that fails to meet matching criteria of a traffic class belongs to the default class. Input policy maps regulate traffic entering the switch module. In an input policy, you can match CoS, DSCP, IP precedence, ACLs, or VLAN IDs and configure individual policing, aggregate policing, or marking to a CoS, DSCP, IP precedence, or QoS group value.

Follow these guidelines when configuring input policy maps:

- You can attach only one input policy map per port.

- The maximum number of policy maps configured on the switch module is 256.
- The number of configurable policer profiles on the switch module is 256. The number of supported policer instances on the switch module is 1,024 minus 1 more than the number of interfaces on the switch module.

  The number of policer instances for the Copper model (GRWIC-D-2S-8PC), which has 10 interfaces, is 1,013; the number of policer instances for the SFP model (GRWIC-D-6S), which has 6 interfaces, is 1,017.

  You can use a policer profile in multiple instances.
- The maximum number of classes in each input policy map is 64 plus **class-default**.
- The number of input policy maps that can be attached in a switch module is limited by the availability of hardware resources. If you attempt to attach an input policy map that causes any hardware resource limitation to be exceeded, the configuration fails.
- After you have attached a single-level policy map to an interface by using the **service-policy input** interface configuration command, you can modify the policy without detaching it from the interface. You can add or delete classification criteria, add or delete classes, add or delete actions, or change the parameters of the configured actions (policers, rates, mapping, marking, and so on). This also applies to changing criteria for the child policy of a hierarchical policy map, as in a per-port per-VLAN hierarchical policy map.

  For the parent policy of a hierarchical policy map, you cannot add or delete a class at the parent level if the policy map is attached to an interface. You must detach the policy from the interface, modify the policy, and then re-attach it to the interface.
- You can configure a maximum 2-level hierarchical policy map as an input policy map only with VLAN-based classification at the parent level and no VLAN-based classification at the child level.
- When an input policy map with only Layer 2 classification is attached to a routed port or a switch module port containing a routed SVI, the service policy acts only on switching eligible traffic and not on routing eligible traffic.
- On an 802.1Q tunnel port, you can use only an input policy map with Layer 2 classification based on MAC ACLs to classify traffic. Input policy maps with Layer 3 classification or with Layer 2 classification based on CoS or VLAN ID are not supported on tunnel ports.
- Input policy maps support policing and marking, not scheduling or queuing. You cannot configure **bandwidth**, **priority**, **queue-limit**, or **shape average** in input policy maps.

These sections describe how to configure different types of input policy maps:

- Configuring Input Policy Maps with Individual Policing, page 14-48
- Configuring Input Policy Maps with Aggregate Policing, page 14-54
- Configuring Input Policy Maps with Marking, page 14-58
- Configuring Per-Port Per-VLAN QoS with Hierarchical Input Policy Maps, page 14-59

Configuring Input Policy Maps with Individual Policing

You use the **police** policy-map class configuration command to configure individual policers to define the committed rate limitations, committed burst size limitations of the traffic, and the action to take for a class of traffic.

Follow these guidelines when configuring individual policers:

- Policing is supported only on input policy maps.

- The switch module supports a maximum of 229 policers. (228 user-configurable policers and 1 policer reserved for internal use).
- When CPU protection is enabled (the default), you can configure 45 ingress policers per port. If you disable CPU protection by entering the **no policer cpu uni all** global configuration command and reloading the switch module, you can configure a maximum of 63 policers per port for user-defined classes and one for class-default. You can enter the **show policer cpu uni-eni** {**drop** | **rate**} privileged EXEC command to see if CPU protection is enabled.
- When you use a table map for police exceed-action in an input policy map, the protocol type of the *map from* type of action must be the same as the protocol type of the associated classification. For example, if the associated class map represents an IP classification, the **map from** type of action that references the table map must be **dscp** or **precedence**. If the associated class map represents a non-IP classification, the **map from** type of action that references the table map must be **cos**.
- 2-rate, 3-color policing is supported only on input policy maps; 1-rate, 2-color policing is supported on both input and output policy maps.
- The number of policer instances on the switch module can be 1024 minus 1 more than the number interfaces. The switch module supports a maximum of 256 policer profiles.
- If you do not configure a violate-action, by default the violate class is assigned the same action as the exceed-action.

If you enter the **no** policy-map configuration command or the **no policy-map** *policy-map-name* global configuration command to delete a policy map that is attached to an interface, a warning message appears that lists any interfaces from which the policy map is being detached. The policy map is then detached and deleted. For example:

```
Warning: Detaching Policy test1 from Interface GigabitEthernet0/1
```

Beginning in privileged EXEC mode, follow these steps to create an input policy map with individual 2-rate, 3-color policing:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Create a policy map by entering the policy map name, and enter policy-map configuration mode. By default, no policy maps are defined.	**policy-map** *policy-map-name*
Step 3	Enter a class-map name or **class-default** to match all unclassified packets, and enter policy-map class configuration mode. If you enter a class-map name, you must have already created the class map by using the **class-map** global configuration command.	**class** {*class-map-name* | **class-default**}

Step	Command
Step 4 Define a policer using one or two rates—committed information rate (CIR) and peak information rate (PIR) for the class of traffic. By default, no policer is defined. • For *rate-bps,* specify average traffic rate in bits per second (bps). The range is 8000 to 1000000000. • For **cir** *cir-bps,* specify a committed information rate at which the bc token bucket is updated in bits per second (b/s). The range is 8000 to 1000000000. • For *burst-bytes* (optional), specify the normal burst size in bytes. The range is 8000 to 1000000. • (Optional) For **bc** *conform-burst,* specify the conformed burst used by the bc token bucket for policing.The range is 8000 to 1000000 bytes. • (Optional) For **pir** *pir-bps,* specify the peak information rate at which the be token bucket for policing is updated. The range is 8000 to 1000000000 b/s. If you do not enter a **pir** *pir-bps*, the policer is configured as a 1-rate, 2-color policer. • For **be** *peak-burst*, specify the peak burst size used by the be token bucket. The range is 8000 to 1000000 bytes. The default is internally calculated based on the user configuration.	**police** {*rate-bps* | **cir** {*cir-bps*} [*burst-bytes*] [**bc** [*conform-burst*] [**pir** *pir-bps* [**be** *peak-burst*]]

	Step	Command
Step 5	(Optional) Enter the action to be taken on packets, depending on whether or not they conform to the CIR and PIR. • (Optional) For **conform-action**, specify the action to perform on packets that conform to the CIR and PIR. The default is **transmit**. • (Optional) For **exceed-action**, specify the action to perform on packets that conform to the PIR but not the CIR. The default is **drop**. • (Optional) For **violate-action**, specify the action to perform on packets that exceed the PIR. The default is **drop**. • (Optional) For *action*, specify one of these actions to perform on the packets: – **drop**—Drop the packet. **Notes:** If the conform action is set to **drop**, the exceed and violate actions are automatically set to **drop**. If the exceed action is set to **drop**, the violate action is automatically set to **drop**. • **set-cos-transmit** *cos-value*—Enter a new CoS value to be assigned to the packet, and send the packet. The range is from 0 to 7. • **set-dscp-transmit** *dscp-value*—Enter a new IP DSCP value to be assigned to the packet, and send the packet. The range is from 0 to 63. You can also enter a mnemonic name for a commonly used value. • **set-prec-transmit** *cos-value*—Enter a new IP precedence value to be assigned to the packet, and send the packet. The range is from 0 to 7. • **set-qos-transmit** *qos-group-value*—Identify a qos-group to be used at egress to specify packets. The range is from 0 to 99. • **transmit**—Send the packet without altering it. You can enter a single conform-action as part of the command string following the police command. You can also press Enter after the **police** command to enter policy-map class police configuration mode, where you can enter multiple actions. In policy-map class police configuration mode, you must enter an action to take.	**conform-action** [**drop** | **set-cos-transmit** {*cos_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*dscp_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*precedence_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group_value* | **transmit**] | **exceed-action** [**drop** | **set-cos-transmit** {*cos_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*dscp_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*precedence_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group_value* | **transmit**] | **violate- action** [**drop** | **set-cos-transmit** {*cos_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*dscp_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*precedence_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group_value* | **transmit**]
Step 6	Return to policy-map configuration mode.	**exit**
Step 7	Return to global configuration mode.	**exit**

	Step	Command
Step 8	Enter interface configuration mode for the interface to which you want to attach the policy.	**interface** *interface-id*
Step 9	Attach the policy map (created in Step 2) to the ingress interface.	**service-policy input** *policy-map-name*
Step 10	Return to privileged EXEC mode.	**end**
Step 11	Verify your entries.	**show policy-map** [*policy-map-name*| **interface**]
Step 12	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

After you have created an input policy map, you attach it to an interface in the input direction. See the "Attaching a Traffic Policy to an Interface" section on page 14-47.

Use the **no** form of the appropriate command to delete an existing policy map, class map, or policer.

This example shows how to configure 2-rate, 3-color policing using policy-map configuration mode:

```
Switch(config)# class-map cos-4
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map in-policy
Switch(config-pmap)# class cos-4
Switch(config-pmap-c)# police cir 5000000 pir 8000000 conform-action transmit
exceed-action set-dscp-transmit 24 violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input in-policy
Switch(config-if)# exit
```

This example shows how to create the same configuration using policy-map class police configuration mode:

```
Switch(config)# class-map cos-4
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map in-policy
Switch(config-pmap)# class cos-4
Switch(config-pmap-c)# police cir 5000000 pir 8000000
Switch(config-pmap-c-police)# conform-action transmit
Switch(config-pmap-c-police)# exceed-action set-dscp-transmit 24
Switch(config-pmap-c-police)# violate-action drop
Switch(config-pmap-c-police)# end
```

This example shows how to create a traffic classification with a CoS value of 4, create a policy map, and attach it to an ingress port. The average traffic rate is limited to 10000000 b/s with a burst size of 10000 bytes:

```
Switch(config)# class-map video-class
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map video-policy
Switch(config-pmap)# class video-class
Switch(config-pmap-c)# police 10000000 10000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
```

```
Switch(config-if)# service-policy input video-policy
Switch(config-if)# exit
```

This example shows how to create policy map with a conform action of **set dscp** and a default exceed action:

```
Switch(config)# class-map in-class-1
Switch(config-cmap)# match dscp 14
Switch(config-cmap)# exit
Switch(config)# policy-map in-policy
Switch(config-pmap)# class in-class-1
Switch(config-pmap-c)# police 230000 8000 conform-action set-dscp-transmit 33
exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input in-policy
Switch(config-if)# exit
```

This example shows how to use policy-map class police configuration mode to set multiple conform actions and an exceed action. The policy map sets a committed information rate of 23000 bits per second (bps) and a conform burst size of 10000 bytes. The policy map includes multiple conform actions (for DSCP and for Layer 2 CoS) and an exceed action:

```
Switch(config)# class-map cos-set-1
Switch(config-cmap)# match cos 3
Switch(config-cmap)# exit
Switch(config)# policy-map map1
Switch(config-pmap)# class cos-set-1
Switch(config-pmap-c)# police cir 23000 bc 10000
Switch(config-pmap-c-police)# conform-action set-dscp-transmit 48
Switch(config-pmap-c-police)# conform-action set-cos-transmit 5
Switch(config-pmap-c-police)# exceed-action drop
Switch(config-pmap-c-police)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input map1
Switch(config-if)# exit
```

This example shows how to use policy-map class police configuration mode to set exceed action mark-down using table-maps. The policy map sets a committed information rate of 23000 bps and a conform burst-size of 10000 bytes. The policy map includes the default conform action (**transmit**) and the exceed action to mark the Layer 2 CoS value based on the table map and to mark IP DSCP to af41:

```
Switch(config)# policy-map in-policy
Switch(config-pmap)# class in-class-1
Switch(config-pmap-c)# police cir 23000 bc 10000
Switch(config-pmap-c-police)# exceed-action set-cos-transmit cos table
police-cos-markdn-tablemap
Switch(config-pmap-c-police)# exceed-action set-dscp-transmit af41
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input in-policy
Switch(config-if)# exit
```

Configuring Input Policy Maps with Aggregate Policing

You use the **policer aggregate** global configuration command to configure an aggregate policer. An aggregate policer is shared by multiple traffic classes within the same policy map. You define the aggregate policer, create a policy map, associate a class map with the policy map, associate the policy map with the aggregate policer, and apply the service policy to a port.

Follow these guidelines when configuring aggregate policers:

- Aggregate policing is supported only on input policy maps.
- The switch module supports a maximum of 229 policers associated with ports (228 user-configurable policers and 1 policer reserved for internal use). You can configure up to 45 policers on a port.
- When CPU protection is enabled (the default), you can configure 45 ingress policers per port. If you disable CPU protection by entering the **no policer cpu uni all** global configuration command and reloading the switch module, you can configure a maximum of 63 policers per port for user-defined classes and one for class-default. You can enter the **show policer cpu uni-eni** {**drop** | **rate**} privileged EXEC command to see if CPU protection is enabled.
- The maximum number of configured aggregate policers is 256.
- The number of policer instances on the switch module can be 1024 minus 1 more than the total number interfaces on the switch module. The switch module supports a maximum of 256 policer profiles.
- If you do not configure a violate-action, by default the violate class is assigned the same action as the exceed-action.
- Only one policy map can use any specific aggregate policer. Aggregate policing cannot be used to aggregate streams across multiple interfaces. You can use aggregate policing only to aggregate streams across multiple classes in a policy map attached to an interface and to aggregate traffic streams across VLANs on a port in a per-port, per-VLAN policy map.
- When you use a table map for police exceed-action in an input policy map, the protocol type of the map from type of action must be the same as the protocol type of the associated classification. For example, if the associated class map represents an IP classification, the **map from** type of action that references the table map must be either **dscp** or **precedence**. If the associated class map represents a non-IP classification, the **map from** type of action that references the table map must be **cos**.
- Table maps are not supported for violate-action for aggregate policing unless a table map is configured for **exceed-action** and no explicit action is configured for **violate-action**.

You can configure multiple conform, exceed, and violate actions simultaneously for an aggregate policer as parameters in the **policer aggregate** global configuration command, but you must enter the actions in this order:

- **conform-action** must be followed by **drop** or **transmit** or by **set** actions in this order:

  set-qos-transmit

  set-dscp-transmit or **set-prec-transmit**

  set-cos-transmit

- **exceed-action** must be followed by **drop** or **transmit** or by **set** actions in this order:

  set-qos-transmit

  set-dscp-transmit or **set-prec-transmit**

  set-cos-transmit

- **violate-action** must be followed by **drop** or **transmit** or by **set** actions in this order:
  - **set-qos-transmit**
  - **set-dscp-transmit or set-prec-transmit**
  - **set-cos-transmit**

Note You do not configure aggregate policer conform-action, exceed-action, and violate-action in policy-map class police configuration mode—you must enter all actions in a string. Consequently, if you enter multiple conform, exceed, and violate actions, the command can become quite long, in which case it might be truncated and difficult to read.

Beginning in privileged EXEC mode, follow these steps to create a 2-rate, 3-color aggregate policer:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Define the policer parameters that can be applied to multiple traffic classes within the same policy map. • For *aggregate-policer-name*, specify the name of the aggregate policer. • For *rate-bps,* specify average traffic rate in bits per second (b/s). The range is 8000 to 1000000000. • For **cir** *cir-bps,* specify a committed information rate (CIR) at which the first token bucket is updated in bits per second (b/s). The range is 8000 to 1000000000. • For *burst-bytes* (optional), specify the normal burst size in bytes. The range is 8000 to 1000000. • (Optional) For **bc** *conform-burst,* specify the conformed burst used by the first token bucket for policing.The range is 8000 to 1000000 bytes.	**policer aggregate** *aggregate-policer-name* {*rate-bps* | **cir** *cir-bps*} [*burst-bytes*] [**bc** [*conform-burst*] [**pir** *pir-bps* [**be** *peak-burst*]] [**conform-action** [**drop** | **set-cos-transmit** {*cos_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*dscp_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*precedence_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group_value* | **transmit**] [**exceed-action** [**drop** | **set-cos-transmit** {*cos_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*dscp_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*precedence_value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group_value* | **transmit**]] [**violate- action** [**drop** | **set-cos-transmit** {*cos_value* | [**cos** | **dscp** | **precedence**]} | **set-dscp-transmit** {*dscp_value* | [**cos** | **dscp** | **precedence**]} | **set-prec-transmit** {*precedence_value* | [**cos** | **dscp** | **precedence**]} | **set-qos-transmit** *qos-group_value* | **transmit**]]

	Step	Command
	• (Optional) For **pir** *pir-bps,* specify the peak information rate at which the second token bucket for policing is updated. The range is 8000 to 1000000000 bits per second. If you do not enter a **pir** *pir-bps*, the policer is configured as a 1-rate, 2-color policer. • For **be** *peak-burst*, specify the peak burst size used by the second token bucket. The range is 8000 to 1000000 bytes. The default is internally calculated based on the user configuration. • (Optional) For **conform-action**, specify the action to take on packets that conform to the CIR. The default is to send the packet. **Note** If the conform action is set to **drop**, the exceed and violate actions are automatically set to **drop**. If the exceed action is set to **drop**, the violate action is automatically set to **drop**. • (Optional) For **exceed-action**, specify the action to take on packets that exceed the CIR. The default is to drop the packet. • (Optional) For **violate-action**, specify the action to take on packets that exceed the CIR. The default is to drop the packet. For definitions of the action keywords, see the command reference for this release or the "Configuring Input Policy Maps with Individual Policing" section on page 14-48. **Note** You cannot configure table maps for **violate-action** for aggregate policing unless a table map is configured for **exceed-action** and no explicit action is configured for violate-action.	
Step 3	Create a policy map by entering the policy map name, and enter policy-map configuration mode.	**policy-map** *policy-map-name*
Step 4	Enter a class-map name or **class-default** to match all unclassified packets, and enter policy-map class configuration mode. If you enter a class-map name, you must have already created the class map by using the **class-map** global configuration command.	**class** {*class-map-name* | **class-default**}
Step 5	Apply an aggregate policer to multiple classes in the same policy map. For *aggregate-policer-name*, enter the name specified in Step 2.	**police aggregate** *aggregate-policer-name*

	Step	Command
Step 6	Return to policy-map configuration mode.	**exit**
Step 7	Return to global configuration mode.	**exit**
Step 8	Enter interface configuration mode for the interface to which you want to attach the policy.	**interface** *interface-id*
Step 9	Attach the policy map (created in Step 3) to the ingress interface.	**service-policy input** *policy-map-name*
Step 10	Return to privileged EXEC mode.	**end**
Step 11	Verify your entries.	**show policer aggregate** [*aggregate-policer-name*]
Step 12	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

After you have created an aggregate policer, you attach it to an ingress port. See the "Attaching a Traffic Policy to an Interface" section on page 14-47.

To remove the specified aggregate policer from a policy map, use the **no police aggregate** *aggregate-policer-name* policy map configuration mode. To delete an aggregate policer and its parameters, use the **no policer aggregate** *aggregate-policer-name* global configuration command.

This example shows how to create an aggregate policer and attach it to multiple classes within a policy map. The policy map is attached to an ingress port:

```
Switch(config)# policer aggregate example 10900000 80000 conform-action transmit
exceed-action drop
Switch(config)# class-map testclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map testclass2
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
Switch(config)# policy-map testexample
Switch(config-pmap)# class testclass
Switch(config-pmap-c)# police aggregate example
Switch(config-pmap-c)# exit
Switch(config-pmap)# class testclass2
Switch(config-pmap-c)# police aggregate example
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input testexample
Switch(config-if)# exit
```

This example shows how to create a 2-rate, 3-color aggregate policer and attach it to multiple classes within a policy map. The policy map is attached to an ingress port:

```
Switch(config)# policer aggregate example cir 10900000 pir 80000000 conform-action
transmit exceed-action drop violate-action drop
Switch(config)# class-map testclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map testclass2
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
Switch(config)# policy-map testexample
```

```
Switch(config-pmap)# class testclass
Switch(config-pmap-c)# police aggregate example
Switch(config-pmap-c)# exit
Switch(config-pmap)# class testclass2
Switch(config-pmap-c)# police aggregate example
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input testexample
Switch(config-if)# exit
```

Configuring Input Policy Maps with Marking

You use the **set** policy-map class configuration command to set or modify the attributes for traffic belonging to a specific class. Follow these guidelines when configuring marking in policy maps:

- You can configure a maximum of 100 QoS groups on the switch module.
- When you use a table map for marking in an input policy map, the protocol type of the map from type of action must be the same as the protocol type of the associated classification. For example, if the associated class map represents an IP classification, the **map from** type of action that references the table map must be either **dscp** or **precedence**. If the associated class map represents a non-IP classification, the **map from** type of action that references the table map must be **cos**.

Beginning in privileged EXEC mode, follow these steps to create an input policy map that marks traffic:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Create a policy map by entering the policy map name, and enter policy-map configuration mode.	**policy-map** *policy-map-name*
Step 3	Enter a class-map name, or **class-default** to match all unclassified packets, and enter policy-map class configuration mode. If you enter a class-map name, you must have already created the class map by using the **class-map** global configuration command.	**class** {*class-map-name* | **class-default**}
Step 4	Mark traffic by setting a new value in the packet, specifying a table map, or specifying a QoS group. • For **qos-group** *value,* identify a QoS group to be used at egress to identify specific packets. The range is from 0 to 99. • For **cos** *cos_value,* enter a new CoS value to be assigned to the classified traffic. The range is 0 to 7. • For [**ip**] **dscp** *new-dscp*, enter a new DSCP value to be assigned to the classified traffic. The range is 0 to 63. • For [**ip**] **precedence** *new-precedence,* enter a new IP-precedence value to be assigned to the classified traffic. The range is 0 to 7.	**set qos-group** *value* and/or **set cos** {*cos_value* | **cos** [**table** *table-map-name*] | **dscp** [**table** *table-map-name*] | **precedence** [**table** *table-map-name*]} and/or **set** [**ip**] **dscp** {*dscp_value* | **cos** [**table** *table-map-name*] | **dscp** [**table** *table-map-name*] | **precedence** [**table** *table-map-name*]} and/or **set** [**ip**] **precedence** {*precedence_value* | **cos** [**table** *table-map-name*] | **dscp** [**table** *table-map-name*] | **precedence** [**table** *table-map-name*]}

	Step	Command
	• You can also configure a CoS, DSCP, or IP precedence table and optionally enter the table name. If you do not enter **table** *table-map name*, the table map default behavior is **copy**. See the "Configuring Table Maps" section on page 14-45.	
Step 5	Return to policy-map configuration mode.	**exit**
Step 6	Return to global configuration mode.	**exit**
Step 7	Enter interface configuration mode for the interface to which you want to attach the policy.	**interface** *interface-id*
Step 8	Attach the policy map (created in Step 2) to the ingress interface.	**service-policy input** *policy-map-name*
Step 9	Return to privileged EXEC mode.	**end**
Step 10	Verify your entries.	**show policy-map** [*policy-map-name* [**class** *class-map-name*]]
Step 11	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

Use the **no** form of the appropriate command to delete a policy map or table map or remove an assigned CoS, DSCP, precedence, or QoS-group value.

This example uses a policy map to remark a packet. The first marking (the **set** command) applies to the QoS default class map that matches all traffic not matched by class *AF31-AF33* and sets all traffic to an IP DSCP value of 1. The second marking sets the traffic in classes AF31 to AF33 to an IP DSCP of 3:

```
Switch(config)# policy-map Example
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set ip dscp 1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class AF31-AF33
Switch(config-pmap-c)# set ip dscp 3
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input Example
Switch(config-if)# exit
```

Configuring Per-Port Per-VLAN QoS with Hierarchical Input Policy Maps

Per-port, per-VLAN QoS allows classification based on VLAN IDs for applying QoS for frames received on a given interface and VLAN. This is achieved by using a hierarchical policy map, with a parent policy and a child policy.

Note these guidelines and limitations when configuring per-port, per-VLAN QoS:

- The feature is supported only by using a two-level hierarchical input policy map, where the parent level defines the VLAN-based classification, and the child level defines the QoS policy to be applied to the corresponding VLAN or VLANs.

- You can configure multiple service classes at the parent level to match different combinations of VLANs, and you can apply independent QoS policies to each parent-service class using any child policy map
- A policy is considered a parent policy map when it has one or more of its classes associated with a child policy map. Each class within a parent policy-map is called a parent-class. In parent classes, you can configure only the **match vlan** class-map configuration command. You cannot configure the **match vlan** command in classes within the child policy map.
- A per-port, per-VLAN parent level class map supports only a child-policy association; it does not allow any actions to be configured. For a parent-level class map, you cannot configure an action or a child-policy association for the class **class-default**.
- You cannot configure a mixture of Layer 2 and Layer 3 class maps in a child policy map. When you attempt to associate such a child policy map with a parent policy, the configuration is rejected. However, you can associate Layer 2 child policies and Layer 3 child policies with different parent-level class maps.
- Per-port, per-VLAN QoS is supported only on 802.1Q trunk ports.
- When the child policy-map attached to a VLAN or set of VLANs contains only Layer 3 classification (**match ip dscp**, **match ip precedence**, **match IP ACLs**), take care to ensure that these VLANs are not carried on any other port besides the one on which the per-port, per-vlan policy is attached. Not following this rule could result in improper QoS behavior for traffic ingressing the switch module on these VLANs.
- We also recommend that you restrict VLAN membership on the trunk ports to which the per-port, per-VLAN is applied by using the **switchport trunk allowed vlan** interface configuration command. Overlapping VLAN membership between trunk ports that have per-port, per-VLAN policies with Layer 3 classification could also result in unexpected QoS behavior.

Configuring per-port, per-VLAN QoS includes these tasks:

- Creating Child-Policy Class Maps, page 14-61
- Creating Parent-Policy Class Maps, page 14-63
- Creating Child Policy Maps, page 14-63
- Creating a Parent Policy Map, page 14-64
- Attaching a Parent Policy Map to an Interface, page 14-64

Creating Child-Policy Class Maps

Beginning in privileged EXEC mode, follow these steps to create one or more child-policy class maps:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Create a class map, and enter class-map configuration mode. By default, no class maps are defined. • (Optional) Use the **match-all** keyword to perform a logical-AND of all matching statements under this class map. All match criteria in the class map must be matched. • (Optional) Use the **match-any** keyword to perform a logical-OR of all matching statements under this class map. One or more match criteria must be matched. • For *class-map-name*, specify the name of the class map. If no matching statements are specified, the default is **match-all**. **Note** A **match-all** class map cannot have more than one classification criterion (match statement).	**class-map** [**match-all** | **match-any**] *child-class-map-name*

	Step	Command
Step 3	Define the match criterion to classify traffic. By default, no match criterion is defined. Only one match type per class map is supported, and only one ACL per class map is supported. • For **access-group** *acl-index-or-name,* specify the number or name of an ACL. Matching access groups is supported only in input policy maps. • For **cos** *cos-list*, enter a list of up to four CoS values in a single line to match against incoming packets. Separate each value with a space. You can enter multiple *cos-list* lines to match more than four CoS values. The range is 0 to 7. • For **ip dscp** *dscp-list*, enter a list of up to eight IPv4 DSCP values to match against incoming packets. Separate each value with a space. You can enter multiple *dscp-list* lines to match more than eight DSCP values. The numerical range is 0 to 63. You can also configure DSCP values in other forms. See the "Classification Based on IP DSCP" section on page 14-8. • For **ip precedence** *ip-precedence-list*, enter a list of up to four IPv4 precedence values to match against incoming packets. Separate each value with a space. You can enter multiple *ip-precedence-list* lines to match more than four precedence values. The range is 0 to 7. • For **qos-group** *value,* specify the QoS group number. The range is 0 to99. Matching of QoS groups is supported only in output policy maps. • For **vlan** *vlan-list,* specify a VLAN ID or a range of VLANs to be used in a parent policy map for per-port, per-VLAN QoS on a trunk port. The VLAN ID range is 1 to 4094.	**match** {**access-group** *acl-index-or-name* | **cos** *cos-list* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list* | **qos-group** *value* | **vlan** *vlan-list*}
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entries.	**show class-map**
Step 6	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

Creating Parent-Policy Class Maps

Beginning in privileged EXEC mode, follow these steps to create one or more parent-policy class maps:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Create a **match-any** class map for the parent policy, and enter class-map configuration mode. **Note** You can enter **match-all** or not enter either **match-any** or **match-all** (to default to **match-all**) if you are going to match only one VLAN ID.	**class-map match-any** *parent-class-map-name*
Step 3	Define the VLAN or VLANs on which to classify traffic. For *vlan-id,* specify a VLAN ID, a series of VLAN IDs separated by a space, or a range of VLANs separated by a hyphen to be used in a parent policy map for per-port, per-VLAN QoS on a trunk port. The VLAN ID range is 1 to 4094. You can also enter the **match vlan** command multiple times to match multiple VLANs.	**match vlan** *vlan-id*
Step 4	Return to privileged EXEC mode.	**end**
Step 5	Verify your entries.	**show class-map**
Step 6	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

Creating Child Policy Maps

Beginning in privileged EXEC mode, follow these steps to create one or more child policy maps:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Create a child policy map by entering the policy map name, and enter policy-map configuration mode.	**policy-map** *child-policy-map-name*
Step 3	Enter a child class-map name or **class-default** to match all unclassified packets, and enter policy-map class configuration mode.	**class** {*child-class-map-name* | **class-default**}
Step 4	Use the **police** policy-map class configuration command to configure policers and the action to take for a class of traffic, or use the **set** policy-map class configuration command to mark traffic belonging to the class.	
Step 5	Return to privileged EXEC mode.	**end**

	Step	Command
Step 6	Verify your entries.	**show policy-map** [*child- policy-map-name* [**class** *class-map-name*]]
Step 7	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

Creating a Parent Policy Map

Beginning in privileged EXEC mode, follow these steps to create a parent policy map and attach it to an interface:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Create a parent policy map by entering the policy map name, and enter policy-map configuration mode.	**policy-map** *parent-policy-map-name*
Step 3	Enter the parent class-map name, and enter policy-map class configuration mode.	**class** *parent-class-map-name*
Step 4	Associate the child policy map with the parent policy map	**service policy** *child-policy-map-name*
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Verify your entries.	**show policy-map** [*parent-policy-map-name* [**class** *class-map-name*]]
Step 7	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

Attaching a Parent Policy Map to an Interface

Beginning in privileged EXEC mode, follow these steps to create attach the parent policy map to an interface:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter interface configuration mode for the interface to which you want to attach the policy.	**interface** *interface-id*
Step 3	Configure the port as a trunk port.	**switchport mode trunk**
Step 4	(Recommended) Restrict VLAN membership for trunk ports to avoid overlapping VLAN membership if the per-port, per-VLAN policy includes Layer 3 classification.	**switchport trunk allowed vlan** *vlan-list*
Step 5	Attach the parent policy map (created in the previous section) to the ingress interface.	**service-policy input** *parent- policy-map-name*

	Step	Command
Step 6	Return to privileged EXEC mode.	**end**
Step 7	Verify your entries.	**show policy-map interface** [*interface-id*]
Step 8	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

This is an example of using multiple parent classes to classify matching criteria for voice and video on customer VLANs:

```
Switch(config)# class-map match-any video
Switch(config-cmap)# match ip dscp af41
Switch(config-cmap)# exit
Switch(config)# class-map match-any voice
Switch(config-cmap)# match ip dscp ef
Switch(config-cmap)# exit

Switch(config)# class-map match-any customer1-vlan
Switch(config-cmap)# match vlan 100-105
Switch(config-cmap)# exit
Switch(config)# class-map match-any customer2-vlan
Switch(config-cmap)# match vlan 110-120
Switch(config-cmap)# exit

Switch(config)# policy-map child-policy-1
Switch(config-pmap)# class voice
Switch(config-pmap-c)# police cir 10000000 bc 50000
Switch(config-pmap-c-police)# conform-action set-cos-transmit 5
Switch(config-pmap-c-police)# exceed-action drop
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video
Switch(config-pmap-c)# set cos 4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set cos 0
Switch(config-pmap-c)# exit

Switch(config)# policy-map child-policy-2
Switch(config-pmap)# class voice
Switch(config-pmap-c)# police cir 5000000
Switch(config-pmap-c-police)# conform-action set-cos-transmit 5
Switch(config-pmap-c-police)# exceed-action drop
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video
Switch(config-pmap-c)# police cir 40000000
Switch(config-pmap-c-police)# conform-action set-cos-transmit 4
Switch(config-pmap-c-police)# exceed-action set-cos-transmit 1
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set cos 0
Switch(config-pmap-c)# exit

Switch(config)# policy-map uni-parent
Switch(config-pmap)# class customer1-vlan
Switch(config-pmap-c)# service-policy child-policy-1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class customer2-vlan
```

```
Switch(config-pmap-c)# service-policy child-policy-2
Switch(config-pmap-c)# exit

Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 100-105, 110-120
Switch(config-if)# service-policy input uni-parent
Switch(config-pmap-c)# exit
```

Configuring Output Policy Maps

You use output policy maps to manage congestion avoidance, queuing, and scheduling of packets leaving the switch module. The switch module has four egress queues, and you use output policy maps to control the queue traffic. You configure shaping, queue-limit, and bandwidth on these queues. You can use high priority (class-based priority queuing). Policing is not supported on output policy maps, except when configuring priority with police for class-based priority queuing. Output policy map classification criteria are matching a CoS, DSCP, or IP precedence value or a QoS group.

Follow these guidelines when configuring output policy maps on physical ports:

- You can configure and attach as many output policy maps as there are ports on the switch module. Multiple output policy maps can use the same queue-limit configuration. However, these policy maps can have only three unique queue-limit configurations.
- Output policy maps can have a maximum of four classes, including the class **class-default**.
- All output policy maps must have the same number of defined class-maps defined, either 1, 2, or 3.
- All output policy maps must use the same set of classes, although the actions for each class can differ for each output policy map.
- In a child policy map, the **class-default** supports all output policy map actions except **priority** and **police**. Action restrictions for **class-default** are the same as for other classes except that a queue limit configuration for **class-default** does not require a scheduling action.
- To classify based on criteria at the output, the criteria must be established at the input. You can establish criteria at the input through classification only when you configure only policing and not marking, or through explicit marking when you configure any marking (policing with **conform** or **exceed** marking or unconditional **set** marking).
- You cannot configure class-based priority queuing under the class **class-default** in an output policy map
- In an output policy map, unless priority queuing is configured, the class default receives a minimum bandwidth guarantee equal to the unconfigured bandwidth on the port.
- After you have attached an output policy map to an interface by using the **service-policy** interface configuration command, you can change only the parameters of the configured actions (rates, percentages, and so on) or add or delete classification criteria of the class map while the policy map is attached to the interface. To add or delete a class or action, you must detach the policy map from all interfaces, modify it, and then reattach it to interfaces.

Note If you anticipate that you might need three classes in a policy map, you should define three classes when you create the policy map, even if you are not ready to use all three at that time. You cannot add a class to a policy map after it has been attached to an interface.

- When at least one output policy map is attached to a active port, other active ports without output policy maps attached might incorrectly schedule and incorrectly order traffic that uses the same classes as the attached output policy maps. We recommend attaching output policy maps to all ports that are in use. We also recommend putting any unused ports in the shutdown state by entering the **shutdown** interface configuration command. For example, if you attach an output policy map that shapes DSCP 23 traffic to a port, DSCP traffic that is sent out of any other port without a policy map attached could be incorrectly scheduled or ordered incorrectly with respect to other traffic sent out of the same port.
- We strongly recommended that you disable port speed autonegotiation when you attach an output policy map to a port to prevent the port from autonegotiating to a rate that would make the output policy map invalid. You can configure a static port speed by using the **speed** interface configuration command. If an output policy-map is configured on a port that is set for autonegotiation and the speed autonegotiates to a value that invalidates the policy, the port is put in the error-disabled state.
- You can attach only one output policy map per port.
- The maximum number of policy maps configured on the switch module is 256.

These sections describe how to configure different types of output policy maps:

- Configuring Output Policy Maps with Class-Based-Weighted-Queuing, page 14-67
- Configuring Output Policy Maps with Class-Based Shaping, page 14-69
- Configuring Output Policy Maps with Port Shaping, page 14-70
- Configuring Output Policy Maps with Class-Based Priority Queuing, page 14-72
- Configuring Output Policy Maps with Weighted Tail Drop, page 14-77

Configuring Output Policy Maps with Class-Based-Weighted-Queuing

You use the **bandwidth** policy-map class configuration command to configure class-based weighted fair queuing (CBWFQ). CBWFQ sets the relative precedence of a queue by allocating a portion of the total bandwidth that is available for the port.

Follow these guidelines when configuring CBWFQ:

- When configuring bandwidth in a policy map, all rate configurations must be in the same format, either a configured rate or a percentage.
- The total rate of the minimum bandwidth guarantees for each queue of the policy cannot exceed the total speed for the interface.
- You cannot configure CBWFQ (**bandwidth**) and traffic (**shape average**) or priority queuing (**priority**) for the same class in an output policy map.
- You cannot configure bandwidth as an absolute rate or a percentage of total bandwidth when strict priority (priority without police) is configured for another class map.
- You can configure bandwidth as a percentage of remaining bandwidth only when strict priority (priority without police) is configured for another class in the output policy map.
- When you configure CIR bandwidth for a class as an absolute rate or a percentage of total bandwidth, any excess bandwidth that remains after servicing the CIR of all classes in the policy map is divided among the classes the same proportion as the CIR rates. If you configure the CIR rate of a class to be 0, that class is not eligible for any excess bandwidth and will receive no bandwidth.

Beginning in privileged EXEC mode, follow these steps to use CBWFQ to control bandwidth allocated to a traffic class by specifying a minimum bandwidth as a bit rate or a percentage:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Create a policy map by entering the policy map name, and enter policy-map configuration mode.	**policy-map** *policy-map-name*
Step 3	Enter a *child class-map name* or **class-default** to match all unclassified packets, and enter policy-map class configuration mode.	**class** {*class-map-name* | **class-default**}
Step 4	Set output bandwidth limits for the policy-map class. • Enter a *rate* to set bandwidth in kilobits per second. The range is from 64 to 1000000. • Enter **percent** *value* to set bandwidth as a percentage of the total bandwidth. The range is 1 to 100 percent. • Enter **remaining percent** *value* to set bandwidth as a percentage of the remaining bandwidth. The range is 1 to 100 percent. This keyword is valid only when strict priority (priority without police) is configured for another class in the output policy map.	**bandwidth** {*rate* | **percent** *value* | **remaining percent** *value*}
	You must specify the same units in each bandwidth configuration in an output policy (absolute rates or percentages). The total guaranteed bandwidth cannot exceed the total available rate.	
Step 5	Return to policy-map configuration mode.	**exit**
Step 6	Return to global configuration mode.	**exit**
Step 7	Enter interface configuration mode for the interface to which you want to attach the policy.	**interface** *interface-id*
Step 8	Attach the policy map (created in Step 2) to the egress interface.	**service-policy output** *policy-map-name*
Step 9	Return to privileged EXEC mode.	**end**
Step 10	Verify your entries.	**show policy-map** [*policy-map-name* [**class** *class-map-name*]]
Step 11	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

After you have created an output policy map, you attach it to an egress port. See the "Attaching a Traffic Policy to an Interface" section on page 14-47.

Use the **no** form of the appropriate command to delete an existing policy map, class map, or bandwidth configuration.

Note If you enter the **no** policy-map configuration command or the **no policy-map** *policy-map-name* global configuration command to delete a policy map that is attached to an interface, a warning message appears that lists any interfaces from which the policy map is being detached. The policy map is then detached and deleted. For example:

```
Warning: Detaching Policy test1 from Interface GigabitEthernet0/1
```

This example shows how to set the precedence of a queue by allocating 25 percent of the total available bandwidth to the traffic class defined by the class map:

```
Switch(config)# policy-map gold_policy
Switch(config-pmap)# class out_class-1
Switch(config-pmap-c)# bandwidth percent 25
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output gold_policy
Switch(config-if)# exit
```

Configuring Output Policy Maps with Class-Based Shaping

You use the **shape average** policy-map class configuration command to configure traffic shaping. Class-based shaping is a control mechanism that is applied to classes of traffic leaving an interface and uses the shape average command to limit the rate of data transmission used for the committed information rate (CIR) for the class.

Follow these guidelines when configuring class-based shaping:

- Configuring a queue for traffic shaping sets the maximum bandwidth or peak information rate (PIR) of the queue. In the switch module, configuring traffic shaping automatically also sets the minimum bandwidth guarantee or CIR of the queue to the same value as the PIR.
- You cannot configure CBWFQ (**bandwidth**) or priority queuing (**priority**) and traffic (**shape average**) for the same class in an output policy map.
- You cannot configure traffic shaping for a traffic class when strict priority (priority without police) is configured for another class within the output policy-map.

Beginning in privileged EXEC mode, follow these steps to use class-based shaping to configure the maximum permitted average rate for a class of traffic:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Create a policy map by entering the policy map name, and enter policy-map configuration mode.	**policy-map** *policy-map-name*
Step 3	Enter a *child class-map name* or **class-default** to match all unclassified packets, and enter policy-map class configuration mode.	**class** {*class-map-name* | **class-default**}
Step 4	Specify the average class-based shaping rate. For *target bps*, specify the average bit rate in bits per second. The range is from 64000 to 1000000000.	**shape average** *target bps*

	Step	Command
Step 5	Return to policy-map configuration mode.	**exit**
Step 6	Return to global configuration mode.	**exit**
Step 7	Enter interface configuration mode for the interface to which you want to attach the policy.	**interface** *interface-id*
Step 8	Attach the policy map (created in Step 2) to the egress interface.	**service-policy output** *policy-map-name*
Step 9	Return to privileged EXEC mode.	**end**
Step 10	Verify your entries.	**show policy-map** [*policy-map-name* [**class** *class-map-name*]]
Step 11	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

After you have created an output policy map, you attach it to an egress port. See the "Attaching a Traffic Policy to an Interface" section on page 14-47.

Use the **no** form of the appropriate command to delete an existing policy map or class map or to delete a class-based shaping configuration.

This example shows how to configure traffic shaping for outgoing traffic on a Fast Ethernet port so that *outclass1*, *outclass2*, and *outclass3* get a maximum of 50, 20, and 10 Mb/s of the available port bandwidth. The class **class-default** gets the remaining bandwidth:

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class classout1
Switch(config-pmap-c)# shape average 50000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class classout2
Switch(config-pmap-c)# shape average 20000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class classout3
Switch(config-pmap-c)# shape average 10000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

Configuring Output Policy Maps with Port Shaping

Port shaping is applied to all traffic leaving an interface. It uses a policy map with only class default when the maximum bandwidth for the port is specified by using the **shape average** command. A child policy can be attached to the class-default in a hierarchical policy map format to specify class-based actions for the queues on the shaped port.

The total of the minimum bandwidth guarantees (CIR) for each queue of the child policy cannot exceed the total port shape rate.

Beginning in privileged EXEC mode, follow these steps to use port shaping to configure the maximum permitted average rate for a class of traffic:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Create a hierarchical policy map by entering the hierarchical policy map name, and enter policy-map configuration mode for the parent policy.	**policy-map** *policy-map-name*
Step 3	Enter a policy-map class configuration mode for the default class.	**class class-default**
Step 4	Specify the average class-based shaping rate. For *target bps*, specify the average bit rate in bits per second. The range is from 4000000 to 1000000000.	**shape average** *target bps*
Step 5	Specify the child policy-map to be used in the hierarchical policy map if required.	**service-policy** *policy-map-name*
Step 6	Return to policy-map configuration mode.	**exit**
Step 7	Return to global configuration mode.	**exit**
Step 8	Enter interface configuration mode for the interface to which you want to attach the policy.	**interface** *interface-id*
Step 9	Attach the parent policy map (created in Step 2) to the egress interface.	**service-policy output** *policy-map-name*
Step 10	Return to privileged EXEC mode.	**end**
Step 11	Verify your entries.	**show policy-map** [*policy-map-name* [**class** *class-map-name*]]
Step 12	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

After you have created the hierarchical output policy map, you attach it to an egress port. See the "Attaching a Traffic Policy to an Interface" section on page 14-47.

Use the **no** form of the appropriate command to delete an existing hierarchical policy map, to delete a port shaping configuration, or to remove the policy map from the hierarchical policy map.

This example shows how to configure port shaping by configuring a hierarchical policy map that shapes a port to 90 Mbps, allocated according to the *out-policy* policy map configured in the previous example:

```
Switch(config)# policy-map out-policy-parent
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 90000000
Switch(config-pmap-c)# service-policy out-policy
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output out-policy-parent
Switch(config-if)# exit
```

Configuring Output Policy Maps with Class-Based Priority Queuing

You can use the **priority** policy-map class configuration command to ensure that a particular class of traffic is given preferential treatment. With strict priority queuing, the priority queue is constantly serviced; all packets in the queue are scheduled and sent until the queue is empty. Excessive use of the priority queues can possibly delay packets in other queues and create unnecessary congestion.

You can configure strict priority queuing (priority without police), or you can configure an unconditional priority policer (priority with police). Follow these guidelines when configuring priority queuing:

- You can associate the **priority** command with a single unique class for all attached output policies on the switch module.
- When you configure a traffic class as a priority queue, you can configure only **police** and **queue-limit** as other queuing actions for the same class. You cannot configure **bandwidth** or **shape average** with priority queues in the same class.
- You cannot associate the **priority** command with the **class-default** of the output policy map.

Configuring Priority Without Police

Follow these guidelines when configuring strict priority queuing (priority without police):

- You cannot configure priority queuing without policing for a traffic class when class-based shaping (**shape average**) or CBWFQ (**bandwidth**) is configured for another class within the output policy-map.
- When you configure priority queuing without policing for a traffic class, you can only configure the other queues for sharing by using the **bandwidth remaining percent** policy-map class configuration command to allocate excess bandwidth. This command does not guarantee the allocated bandwidth, but does ensure the rate of distribution.

Beginning in privileged EXEC mode, follow these Step to configure a strict priority queue:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Create classes for three egress queues. Enter match conditions classification for each class.	**class-map** *class-map-name*
Step 3	Create a policy map by entering the policy map name, and enter policy-map configuration mode.	**policy-map** *policy-map-name*
Step 4	Enter the name of the priority class (created by using the **class-map** global configuration command), and enter policy-map class configuration mode for the priority class.	**class** *class-map-name*
Step 5	Set the strict scheduling priority for this class. **Note** Only one unique class map on the switch module can be associated with a **priority** command. You cannot configure priority along with any other queuing action (**bandwidth** or **shape average**).	**priority**
Step 6	Exit policy-map class configuration mode for the priority class.	**exit**

	Step	Command
Step 7	Enter the name of a nonpriority class, and enter policy-map class configuration mode for that class.	**class** *class-map-name*
Step 8	Set output bandwidth limits for the policy-map class as a percentage of the remaining bandwidth. The range is 1 to 100 percent.	**bandwidth remaining percent** *value*
Step 9	Exit policy-map class configuration mode for the class	**exit**
Step 10	Return to global configuration mode.	**exit**
Step 11	Enter interface configuration mode for the interface to which you want to attach the policy.	**interface** *interface-id*
Step 12	Attach the policy map (created in Step 3) to the egress interface.	**service-policy output** *policy-map-name*
Step 13	Return to privileged EXEC mode.	**end**
Step 14	Verify your entries.	**show policy-map**
Step 15	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

After you have created an output policy map, you attach it to an egress port. See the "Attaching a Traffic Policy to an Interface" section on page 14-47.

Use the **no** form of the appropriate command to delete an existing policy map or class map or to cancel strict priority queuing for the priority class or the bandwidth setting for the other classes.

This example shows how to configure the class *out-class1* as a strict priority queue so that all packets in that class are sent before any other class of traffic. Other traffic queues are configured so that *out-class-2* gets 50 percent of the remaining bandwidth and *out-class3* gets 20 percent of the remaining bandwidth. The class **class-default** receives the remaining 30 percent with no guarantees:

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit
```

Configuring Priority With Police

You can use the priority with police feature and configure an unconditional priority policer to limit the bandwidth used by the priority queue and allocate bandwidth or shape other queues. Follow these guidelines when configuring priority with police:

- You cannot configure a policer committed burst size for an unconditional priority policer even though the keyword is visible in the CLI help. Any configured burst size is ignored when you try to attach the output service policy.
- The allowed police rate range is 64000 to 1000000000 bps, even though the range that appears in the CLI help is 8000 to 1000000000. You cannot attach an output service policy with an out-of-range rate.
- You cannot configure priority with policing for a traffic class when **bandwidth remaining percent** is configured for another class in the same output policy map.
- You can configure 1-rate, 2-color policers for output policies with priority. You cannot configure 2-rate, 3-color policers for output policies.

Beginning in privileged EXEC mode, follow these steps to configure priority with police:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Create classes for three egress queues. Enter match conditions classification for each class.	**class-map** *class-map-name*
Step 3	Create a policy map by entering the policy map name, and enter policy-map configuration mode.	**policy-map** *policy-map-name*
Step 4	Enter the name of the priority class (created by using the **class-map** global configuration command), and enter policy-map class configuration mode for the priority class.	**class** *class-map-name*
Step 5	Configure this class as the priority class. **Note** Only one unique class map on the switch module can be associated with a **priority** command.	**priority**

	Step	Command
Step 6	Define a policer for the priority class of traffic. • For *rate-bps,* specify average traffic rate in bits per second (bps). The range is 64000 to 1000000000. **Note** When you use the **police** command with the **priority** command in an output policy, the police rate range and the CIR range is 64000 to 1000000000 bps, even though the range that appears in the CLI help is 8000 to 1000000000. You cannot attach an output service policy with an out-of-range rate. • For **cir** *cir-bps,* specify a committed information rate (CIR) in bits per second (bps). The range is 64000 to 1000000000. Although visible in the command-line help string, the burst-size option is not supported in output policy maps. You cannot attach an output service policy map that has a configured burst size.	**police** {*rate-bps* | **cir** *cir-bps*}
Step 7	(Optional) Enter the action to be taken on packets that conform to the CIR. If no action is entered, the default action is to send the packet. **Note** You can enter a single conform-action as part of the command string following the **police** command. You can also enter a carriage return after the **police** command and enter policy-map class police configuration mode to enter the conform-action. When the *police* command is configured with priority in an output policy map, only the default conform-action of **transmit** is supported. Although visible in the command-line help string, the other police conform actions are not supported in output policy maps.	**conform-action** [**transmit**]

	Step	Command
Step 8	(Optional) Enter the action to be taken for packets that do not conform to the CIR. If no action is entered, the default action is to drop the packet. **Note** You can enter a single exceed-action as part of the command string following the **police** command. You can also enter a carriage return after the **police** command and enter policy-map class police configuration mode to enter the exceed-action. When the *police* command is configured with priority in an output policy map, only the default exceed-action of **drop** is supported. Although visible in the command-line help string, the other police exceed actions are not supported in output policy maps.	**exceed-action** [**drop**]
Step 9	Exit policy-map class configuration mode for the priority class.	**exit**
Step 10	Enter the name of the first nonpriority class, and enter policy-map class configuration mode for that class.	**class** *class-map-name*
Step 11	Set output bandwidth limits for the policy-map class in kilobits per second (the range is 64 to 1000000) or a percentage of the total bandwidth (the range is 1 to 100 percent) or specify the average class-based shaping rate in bits per second (the range is 64000 to 1000000000).	**bandwidth** {**rate** | **percent** *value*} or **shape average** *target bps*
Step 12	Return to policy-map configuration mode.	**exit**
Step 13	Return to global configuration mode.	**exit**
Step 14	Enter interface configuration mode for the interface to which you want to attach the policy.	**interface** *interface-id*
Step 15	Attach the policy map (created in Step 3) to the egress interface.	**service-policy output** *policy-map-name*
Step 16	Return to privileged EXEC mode.	**end**
Step 17	Verify your entries.	**show policy-map**
Step 18	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

After you have created an output policy map, you attach it to an egress port. See the "Attaching a Traffic Policy to an Interface" section on page 14-47.

Use the **no** form of the appropriate command to delete an existing policy map or class map or to cancel the priority queuing or policing for the priority class or the bandwidth setting for the other classes.

This example shows how to use the **priority** with **police** commands to configure *out-class1* as the priority queue, with traffic going to the queue limited to 20000000 bps so that the priority queue never uses more than that. Traffic above that rate is dropped. The other traffic queues are configured as in the previous example:

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police 200000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit
```

Configuring Output Policy Maps with Weighted Tail Drop

Weighted tail drop (WTD) adjusts the queue size (buffer size) associated with a traffic class. You configure WTD by using the **queue-limit** policy-map class configuration command.

Follow these guidelines when configuring WTD:

- Configuring WTD with the **queue-limit** command is supported only when you first configure a scheduling action, such as **bandwidth**, **shape average**, or **priority**. The exception to this is when you are configuring **queue-limit** in the **class-default**.
- You can configure and attach as many output policy maps as there are ports. Multiple output policy maps can use the same queue-limit configuration. However, these policy maps can have only three unique queue-limit configurations.
- You can use the **queue-limit** command to configure the queue-limit for CPU-generated traffic.
- When you use the **queue-limit** command to configure queue thresholds for a class, the WTD thresholds must be less than or equal to the queue maximum threshold. A queue size configured with no qualifier must be larger than any queue sizes configured with qualifiers.
- You cannot configure more than two unique threshold values for the WTD qualifiers (**cos**, **dscp**, **precedence**, or **qos-group**) in the **queue-limit** command. However, there is no limit to the number of qualifiers that you can map to those thresholds. You can configure a third unique threshold value to set the maximum queue, using the **queue-limit** command with no qualifiers.
- A WTD qualifier in the **queue-limit** command must be the same as at least one **match** qualifier in the associated class map.
- In an output policy map, when you configure a queue-limit for a unique class, all other output policy maps must use the same format of qualifier type and qualifier value. Only queue-limit threshold values can be different. For example, when you configure class A queue-limit thresholds for **dscp 30** and **dscp 50** in *policy-map1*, and you configure class A queue-limits in policy-map 2, you must use **dscp 30** and **dscp 50** as qualifiers. You cannot use **dscp 20** and **dscp 40**. The threshold values can be different, but different threshold values would create a new unique queue-limit configuration.

Beginning in privileged EXEC mode, follow these steps to use WTD to adjust the queue size for a traffic class:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Create a policy map by entering the policy map name, and enter policy-map configuration mode.	**policy-map** *policy-map-name*
Step 3	Enter a child class-map name, or **class-default** to match all unclassified packets, and enter policy-map class configuration mode. • If you enter a class-map name, you must perform Step 4 to configure a scheduling action (**bandwidth**, **shape average**, or **priority**) before you go to Step 5 to configure queue-limit. • If you enter class-default, you can skip Step 4.	**class** {*class-map-name* | **class-default**}
Step 4	Configure a scheduling action for the traffic class. For more information, see: • "Configuring Output Policy Maps with Class-Based-Weighted-Queuing" section on page 14-67 • "Configuring Output Policy Maps with Class-Based Shaping" section on page 14-69 • "Configuring Output Policy Maps with Port Shaping" section on page 14-70 • "Configuring Output Policy Maps with Class-Based Priority Queuing" section on page 14-72.	**bandwidth** {*rate* | **percent** *value* | **remaining percent** *value*} or **shape average** *target bps* or **priority**

	Step	Command
Step 5	Specify the queue size for the traffic class. • (Optional) For **cos** *value*, specify a CoS value. The range is from 0 to 7. • (Optional) For **dscp** *value*, specify a DSCP value. The range is from 0 to 63. • (Optional) For **precedence** *value*, specify an IP precedence value. The range is from 0 to 7. • (Optional) For **qos-group** *value*, enter a QoS group value. The range is from 0 to 99. • For *number-of-packets*, set the minimum threshold for WTD. The range is from 16 to 544, in multiples of 16, where each packet is a fixed unit of 256 bytes. **Note** For optimal performance, we strongly recommend that you configure the queue-limit to 272 or less. The value is specified in packets by default, but the **packets** keyword is optional. **Note** Multiple output policy maps can use the same queue-limit configuration. However these policy maps can have only three unique queue-limit configurations.	**queue-limit** [**cos** *value* | **dscp** *value* | **precedence** *value* | **qos-group** *value*] *number-of-packets* [**packets**]}
Step 6	Return to policy-map configuration mode.	**exit**
Step 7	Return to global configuration mode.	**exit**
Step 8	Enter interface configuration mode for the interface to which you want to attach the policy.	**interface** *interface-id*
Step 9	Attach the policy map (created in Step 2) to the egress interface. **Note** If you try to attach an output policy map that contains a fourth queue-limit configuration, you see an error message, and the attachment is not allowed.	**service-policy output** *policy-map-name*
Step 10	Return to privileged EXEC mode.	**end**
Step 11	Verify your entries.	**show policy-map** [*policy-map-name* [**class** *class-map-name*]]
Step 12	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

After you have created an output policy map, you attach it to an egress port. See the "Configuring Output Policy Maps" section on page 14-66.

Use the **no** form of the appropriate command to delete an existing policy map or class map or to delete a WTD configuration.

This example shows a policy map with a specified bandwidth and queue size. Traffic that is not DSCP 30 or 10 is assigned a queue limit of 112 packets. Traffic with a DSCP value of 30 is assigned a queue-limit of 48 packets, and traffic with a DSCP value of 10 is assigned a queue limit of 32 packets. All traffic not belonging to the class traffic is classified into class-default, which is configured with 10 percent of the total available bandwidth and a large queue size of 256 packets:

```
Switch(config)# policy-map gold-policy
Switch(config-pmap)# class traffic
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# queue-limit 112
Switch(config-pmap-c)# queue-limit dscp 30 48
Switch(config-pmap-c)# queue-limit dscp 10 32
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 256
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output gold-policy
Switch(config-if)# exit
```

Configuring QoS Marking and Queuing for CPU-Generated Traffic

Beginning in privileged EXEC mode, follow these steps to configure marking and queuing of CPU-generated traffic. This procedure is optional.

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Refer to the "Configuring Table Maps" section on page 14-45.	Configure global table maps
Step 3	Mark traffic by setting a new CoS value or by specifying a table map. • For *cos-value*, enter a new CoS value. The range is from 0 to 7. • You can also mark CoS based on the CoS, DSCP, or IP-precedence value. You can optionally use a table map to configure CoS. If you do not enter **table-map** *table-map-name*, the table map default behavior is **copy**. See the "Table Maps" section on page 14-14. When you complete this step, go to Step 7.	**cpu traffic qos cos** {*cos-value* | **cos [table-map** *table-map-name*] | **dscp [table-map** *table-map-name*] | **prec [table-map** *table-map-name*]}

	Step	Command
Step 4	Mark traffic by setting a new DsCP value or by specifying a table map. • For **dscp** *new-dscp*, enter a new DSCP value for the classified traffic. The range is 0 to 63. • You can also configure a table map to mark DSCP based on the CoS, DSCP, or IP-precedence value. You can optionally enter the table name. If you do not enter **table-map** *table-map-map* name, the table map default behavior is **copy**. See the "Table Maps" section on page 14-14. • For additional DSCP classification options, see the "Classification Based on IP DSCP" section on page 14-8. When you complete this step, go to Step 7.	**cpu traffic qos dscp** {*dscp_value* | **cos [table-map** *table-map-name*] | **dscp [table-map** *table-map-name*] | **prec [table-map** *table-map-name*]}
Step 5	Mark traffic by setting a new precedence value or by specifying a table map. • For **precedence** *new-precedence*, enter a new IP-precedence value as a number from 0 to 7 or by name: **routine** (**0**), **priority** (**1**), **immediate** (**2**), **flash** (**3**), **flash-override** (**4**), **critical** (**5**), **internet** (**6**), **network** (**7**). • You can also configure a table map to mark precedence based on the CoS, DSCP, or IP-precedence value. You can optionally enter the table name. If you do not enter **table-map** *table-map-map name*, the table map default behavior is **copy**. See the "Table Maps" section on page 14-14. • When you complete this step, go to Step 7.	**cpu traffic qos precedence** {*precedence_value* | **cos [table-map** *table-map-name*] | **dscp [table-map** *table-map-name*] | **prec** [**table-map** *table-map-name*]}
Step 6	Mark traffic by using a QoS group. For *qos-group-value*, identify a QoS group to use at egress. The range is 0 to 99. When you complete this step, go to Step 7.	**cpu traffic qos qos-group** *qos-group-value*
Step 7	Return to privileged EXEC mode.	**end**
Step 8	Refer to the "Configuring Output Policy Maps" section on page 14-66.	Configure output policy maps to map QoS markings like COS, IP DSCP, IP precedence and QoS group to class queues, configure queuing and scheduling
Step 9	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**
Step 10	Display the configured class maps, policy maps, table maps, and CPU traffic QoS settings.	**show running-config**
Step 11	Display the QoS marking values for CPU-generated traffic.	**show cpu traffic qos**

	Step	Command
Step 12	Display information for all table maps or the specified table map.	**show table-map** [*table-map-name]*
Step 13	Display QoS policy map information for the specified policy map name, interface, input or output policy maps, or policy-map class.	**show policy-map** [*policy-map-name* | **interface** [*interface-id*] [**output**] [**class** *class-name*]]

To disable any command, use the **no** form of the command.

Example 1

This example shows how to configure egress queuing based on the DSCP value of CPU-generated IP packets.

- All CPU-generated IP traffic queues on the egress port, based on its IP DSCP value, and the configured output policy map *output-policy.*
- All IP SLA or TWAMP probes with the DSCP value *ef* to simulate voice traffic are assigned to the *voice* class
- All IP SLA or TWAMP probes with the DSCP values *af41*, *af42* and *af43* to simulate video traffic are assigned to the *video* class
- All IP control protocol traffic with the DSCP values 48 and 56 are assigned to the *network-internetwork-control* class
- The rest of the IP traffic is assigned to the default class
- All CPU-generated non-IP traffic is statically mapped to a fixed queue on the egress port
- All CFM traffic is queued to the default class because there is no class based on CoS

```
Switch(config)# cpu traffic qos dscp dscp
```

Class

```
Switch(config)# class-map match-any video
Switch(config-cmap)# match ip dscp af41 af42 af43
Switch(config-cmap)# exit

Switch(config)# class-map match-any voice
Switch(config-cmap)# match ip dscp ef
Switch(config-cmap)# exit

Switch(config)# class-map match-any network-internetwork-control
Switch(config-cmap)# match ip dscp 48 56
Switch(config-cmap)# exit
```

Policy

```
Switch(config)# policy-map output-policy
Switch(config-pmap)# class voice
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police cir 10000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video
Switch(config-pmap-c)# bandwidth percent 40
Switch(config-pmap-c)# exit
Switch(config-pmap)# class network-internetwork-control
```

```
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 30
Switch(config-pmap-c)# exit
```

Interface

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output output-policy
Switch(config-pmap-c)# exit
```

Example 2

This example shows how to mark the CoS of CPU-generated IP traffic (including IP-SLA and TWAMP) based on the DSCP value in the packet and to configure egress queuing based on the CoS value.

- All CPU-generated IP traffic queues on the egress port, based on the IP DSCP value and the configured output policy map called *output-policy.*
- All IP SLA or TWAMP probes with the DSCP value *ef* to simulate voice traffic are assigned to the *voice* class
- All IP SLA or TWAMP probes with the DSCP values *af41*, *af42* and *af43* to simulate video traffic are assigned to the *video* class
- All IP control protocol traffic with the DSCP values 48 and 56 are assigned to the *network-internetwork-control* class
- The rest of the IP traffic is assigned to the default class
- All CPU-generated non-IP traffic with CoS 5 is assigned to the *voice* class
- All CPU-generated non-IP traffic with CoS 3 is assigned to the *video* class
- All CPU-generated non-IP traffic with CoS 6 and 7 is assigned to the *network-internetwork-control* class
- All CFM traffic with CoS 5 is assigned to the *voice* class
- All CFM traffic with CoS 3 is assigned to the *video* class
- All CFM traffic with CoS 6 and 7 is assigned to the *network-internetwork-control* class

Table Map

```
Switch(config)# table-map dscp-to-cos
Switch(config-tablemap)# map from 46 to 5
Switch(config-tablemap)# map from 48 to 6
Switch(config-tablemap)# map from 56 to 7
Switch(config-tablemap)# map from af41 to 3
Switch(config-tablemap)# map from af42 to 3
Switch(config-tablemap)# map from af43 to 3
Switch(config-tablemap)# default 0
Switch(config-tablemap)# end
```

CPU QoS

```
Switch(config)# cpu traffic qos cos dscp table-map dscp-to-cos
Switch(config)# cpu traffic qos cos cos
```

Class

```
Switch(config)# class-map match-any video
Switch(config-cmap)# match cos 3
Switch(config-cmap)# exit

Switch(config)# class-map match-any voice
Switch(config-cmap)# match cos 5
Switch(config-cmap)# exit

Switch(config)# class-map match-any network-internetwork-control
Switch(config-cmap)# match cos 6 7
Switch(config-cmap)# exit
```

Policy

```
Switch(config)# policy-map output-policy
Switch(config-pmap)# class voice
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police cir 10000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video
Switch(config-pmap-c)# bandwidth percent 40
Switch(config-pmap-c)# exit
Switch(config-pmap)# class network-internetwork-control
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 30
Switch(config-pmap-c)# exit
```

Interface

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output output-policy
Switch(config-pmap-c)# exit
```

Example 3

This example shows how to:

- Mark the DSCP value of CPU-generated IP traffic (including IP-SLA and TWAMP) based on the DSCP value in the packet
- Mark the CoS of CPU-generated IP traffic (including IP-SLA and TWAMP) based on the DSCP value in the packet
- Mark the CoS of CPU-generated non-IP traffic based on the CoS value in the packet.
- Mark all CPU-generated traffic with the QoS group
- Configure egress queuing based on the QoS group

The example has these results:

- All CPU-generated IP traffic with DSCP values 46, 48, and 56 retains the existing markings
- For all other CPU-generated IP packets, the DSCP value is reset to 0
- All CPU-generated IP traffic with DSCP values 46, 48, and 56 is mapped to the corresponding CoS values of 5, 6, and 7 respectively
- For all other CPU-generated IP packets, the CoS value resets to 0

- All CPU-generated non-IP traffic with the CoS values of 5, 6, and 7 retain the existing markings.
- For all other CPU-generated non-IP packets, the CoS value resets to 0
- All CPU-generated traffic goes through a single class called *cpu-traffic*. The *user-voice* classes *user-voice* and *user-video* are reserved for user traffic. As a result, CPU traffic and user traffic are separated into different queues on the egress port.

Table Map

```
Switch(config)# table-map dscp-to-cos
Switch(config-tablemap)# map from 46 to 5
Switch(config-tablemap)# map from 48 to 6
Switch(config-tablemap)# map from 56 to 7
Switch(config-tablemap)# default 0
Switch(config-tablemap)# end

Switch(config)# table-map dscp-to-dscp
Switch(config-tablemap)# map from 46 to 46
Switch(config-tablemap)# map from 48 to 48
Switch(config-tablemap)# map from 56 to 56
Switch(config-tablemap)# default 0
Switch(config-tablemap)# end

Switch(config)# table-map cos-to-cos
Switch(config-tablemap)# map from 5 to 5
Switch(config-tablemap)# map from 6 to 6
Switch(config-tablemap)# map from 7 to 7
Switch(config-tablemap)# default 0
Switch(config-tablemap)# end
```

CPU QoS

```
Switch(config)# cpu traffic qos dscp dscp table-map dscp-to-dscp
Switch(config)# cpu traffic qos cos dscp table dscp-to-cos
Switch(config)# cpu traffic qos cos cos table cos-to-cos
Switch(config)# cpu traffic qos qos-group 50
```

Class

```
Switch(config)# class-map match-any cpu-traffic
Switch(config-cmap)# match qos-group 50
Switch(config-cmap)# exit

Switch(config)# class-map match-any user-video
Switch(config-cmap)# match cos 3
Switch(config-cmap)# exit

Switch(config)# class-map match-any user-voice
Switch(config-cmap)# match cos 5
Switch(config-cmap)# exit
```

Policy

```
Switch(config)# policy-map output-policy
Switch(config-pmap)# class user-voice
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police cir 10000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class user-video
Switch(config-pmap-c)# bandwidth percent 40
```

```
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cpu-traffic
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 30
Switch(config-pmap-c)# exit

Interface

Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output output-policy
Switch(config-pmap-c)# exit
```

Displaying QoS Information

To display QoS information, use one or more of the privileged EXEC commands in Table 14-2. For explanations about available keywords, see the command reference for this release.

Table 14-2 Commands for Displaying QoS Information

Command	Description
show class-map [*class-map-name*]	Display QoS class-map information for all class maps or the specified class map.
show policer aggregate [*aggregate-policer-name*]	Display information about all aggregate policers or the specified aggregate policer.
show policy-map [*policy-map-name* | **interface** [*interface-id*] [**input** | **output**] [**class** *class-name*]]	Display QoS policy map information for the specified policy map name, interface, input or output policy maps, or policy-map class.
show cpu traffic qos	Display the QoS marking values for CPU-generated traffic.
show running-config	Display the configured class maps, policy maps, table maps, and aggregate policers.
show table-map [*table-map-name*]	Display information for all configured table maps or the specified table map.
show class-map [*class-map-name*]	Display QoS class-map information for all class maps or the specified class map.

To test full-path QoS in both directions on an interface, you can configure Ethernet terminal loopback by entering the **ethernet loopback facility** interface configuration command. In terminal loopback mode, the port appears to be up but the link is actually down and no packets are sent out. Configuration changes on the port immediately affect the traffic being looped back. For information about Ethernet terminal loopback, see the “Enabling Ethernet Loopback” section in Chapter 45, “Configuring Ethernet OAM, CFM, and E-LMI” in the *Cisco CGS 2520 Switch Software Configuration Guide*:

http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swoam.html#wp1137522

QoS Statistics

There are several ways to display QoS input and output policy-map statistics.

For input policy maps, you can use the **show policy-map interface** [*interface-id*] privileged EXEC command to display per-class per-policer conform and exceed statistics. Policer conform statistics are the number of packets that conform to the configured policer profile; policer exceed statistics are the number of packets that exceed the configured policer profile. The switch module does not support per-class classification statistics, but you can determine these statistics by configuring policing at line rate for the class. In this case, no packets exceed the configured policer profile, and the policer conform statistics would equal the class classification statistics.

This output also includes byte-level statistics for conform, exceed, and violate classes.

Another way to view input QoS statistics is in the output of the **show platform qos statistics interface** [*interface-id*] privileged EXEC command. The per-port frame statistics are sorted by the DSCP and CoS values of the incoming frames on the port. These statistics do not provide any information about the MQC input policy map configured on the interface.

For output policy maps, you can use the **show policy-map interface** [*interface-id*] command to display per-class classification statistics that show the total number of packets that match the specified class. This count includes the total number of packets that are sent and dropped for that class. You can use the same command to view the per-class tail drop statistics.

Configuration Examples for Policy Maps

This section includes configuration examples for configuring QoS policies on the switch module, including configuration limitations and restrictions. The sections are broken into different configurations actions that a customer might do. Each section provides the exact sequence of steps that you must follow for successful configuration or modification.

- QoS Configuration for Customer A, page 14-87
- QoS Configuration for Customer B, page 14-89
- Modifying Output Policies and Adding or Deleting Classification Criteria, page 14-90
- Modifying Output Policies and Changing Queuing or Scheduling Parameters, page 14-91
- Modifying Output Policies and Adding or Deleting Configured Actions, page 14-92
- Modifying Output Policies and Adding or Deleting a Class, page 14-93

QoS Configuration for Customer A

This section provides examples of the initial configuration and activation of QoS policies for a customer switch module. Input and output QoS service policies are configured based on the requirements and attached to relevant ports.

In the initial configuration for Customer A, Fast Ethernet ports 1 through 24 are user network interfaces (UNIs) and are disabled by default. Gigabit Ethernet ports 1 and 2 are network node interfaces (NNIs) and are enabled by default.

This is the overall sequence for initial configuration:

- Configure classes and policies.
- Shut down all active ports.

- Attach policies to ports to be activated.
- Take the ports out of the shut-down state.
- Leave unused ports shut down.

Note these restrictions for configuring output policies:

- You can define up to three classes in the output policy map.
- The defined classes must be the same as other output policy maps.
- The number of defined classes in each output policy map must be same.
- You must assign an action to each class; that is, there can be no empty class.
- Each class configuration must be based on the classification/marking done in the input policy-map.

This example configures classes for input service policies and defines three classes of service: gold, silver, and bronze. Because a **match-all** classification (the default) can have only single classification criterion, the **match-any** classification is used so that you can add classification criteria in the future:

```
Switch# config terminal
Switch(config)# class-map match-any gold-in
Switch(config-cmap)# match ip dscp af11
Switch(config-cmap)# exit
Switch(config)# class-map match-any silver-in
Switch(config-cmap)# match ip dscp af21
Switch(config-cmap)# exit
Switch(config)# class-map match-any bronze-in
Switch(config-cmap)# match ip dscp af31
Switch(config-cmap)# exit
```

This example shows how to configure an input policy map that marks the gold class and polices the silver class to 50 Mb/s and the bronze class to 20 Mb/s.

```
Switch(config)# policy-map input-all
Switch(config-pmap)# class gold-in
Switch(config-pmap-c)# set ip dscp af43
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver-in
Switch(config-pmap-c)# police 50000000
Switch(config-pmap)# class bronze-in
Switch(config-pmap-c)# police 20000000
Switch(config-pmap-c)# exit
```

This example configures classes for output service policies with three classes of service: gold, silver, and bronze. The gold class is configured to match the marked value in the input service policy. Because a **match-all** classification (the default) can have only single classification criterion, the **match-any** classification is used so that you can add classification criteria in the future.

```
Switch# config terminal
Switch(config)# class-map match-any gold-out
Switch(config-cmap)# match ip dscp af43
Switch(config-cmap)# exit
Switch(config)# class-map match-any silver-out
Switch(config-cmap)# match ip dscp af21
Switch(config-cmap)# exit
Switch(config)# class-map match-any bronze-out
Switch(config-cmap)# match ip dscp af31
Switch(config-cmap)# exit
```

This example configures one output service policy to be applied to both Gigabit Ethernet NNIs, providing priority with rate-limiting to the gold class, class-based shaping for the silver class, and a minimum bandwidth guarantee of 10 percent to the bronze class.

```
Switch(config)# policy-map output-g1-2
Switch(config-pmap)# class gold-out
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police 50000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver-out
Switch(config-pmap-c)# shape average 200000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze-out
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
```

This example configures a second output service policy to be applied to Fast Ethernet UNIs 1 to 8, providing strict priority to the gold class and distributing the remaining bandwidth in the desired proportions over the remaining classes.

```
Switch(config)# policy-map output1-8
Switch(config-pmap)# class gold-out
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver-out
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze-out
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
```

This example attaches the input and output service policies to the Gigabit Ethernet ports and activates them.

```
Switch(config)# interface range gigabitethernet0/1-2
Switch(config-if-range)# service-policy input input-all
Switch(config-if-range)# service-policy output output-g1-2
Switch(config-if-range)# no shutdown
Switch(config-if-range)# exit
```

This example attaches the input and output service policies to Fast Ethernet ports 1 to 8 and activates them.

```
Switch(config)# interface range fastethernet0/1 - 8
Switch(config-if-range)# service-policy input input-all
Switch(config-if-range)# service-policy output output1-8
Switch(config-if-range)# no shutdown
Switch(config-if-range)# exit
```

QoS Configuration for Customer B

This section provides examples for configuring and activating QoS policies on the switch module for a new set of customers without affecting the current customers. Input and output QoS service policies are configured based on the requirements and attached to relevant ports. The example uses an existing input policy-map and configures a new output policy map for the new customers.

In the initial configuration for Customer B, Fast Ethernet ports 1 through 8 are UNIs and are active. Fast Ethernet ports 9 through 24 are UNIs and are shut down. Gigabit Ethernet ports 1 and 2 are NNIs and are enabled by default.

This is the overall sequence of initial configuration:

- Define any new required output policies
- Attach input and output policies to ports to be activated
- Take the ports out of the shut-down state

Note these restrictions when configuring output policies:

- You can define up to three classes in the output policy map
- The defined classes must be the same as other output policy maps
- The number of defined classes in each output policy map must be same
- You must assign an action to each class; that is, there can be no empty class
- Each class configuration must be based on the classification/marking done in the input policy-map.

This example configures a third output service policy to be attached to Fast Ethernet UNIs 9 through 12, providing a minimum guaranteed bandwidth of 50 Mb/s to the gold class, 20 Mb/s to the silver class, and 10 Mb/s to the bronze class:

```
Switch(config)# policy-map output9-12
Switch(config-pmap)# class gold-out
Switch(config-pmap-c)# bandwidth 50000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver-out
Switch(config-pmap-c)# bandwidth 20000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze-out
Switch(config-pmap-c)# bandwidth 10000
Switch(config-pmap-c)# exit
```

This example attaches the output policy for Fast Ethernet ports 9 through 12 and activates the ports:

```
Switch# config terminal
Switch(config)# interface range fastethernet0/9-12
Switch(config-if-range)# service-policy input input-all
Switch(config-if-range)# service-policy output output9-12
Switch(config-if-range)# no shutdown
Switch(config-if-range)# exit
```

Modifying Output Policies and Adding or Deleting Classification Criteria

This section provides examples of updating an existing set of output policy maps to add or delete classification criteria. The modification might be required due to a change in the service provisioning requirements or a change in the input service policy map. You can make the change without shutting down any port.

In the initial configuration, Fast Ethernet ports 1 through 12 are UNIs and are active. Fast Ethernet ports 13 through 24 are UNIs and are shut down. Gigabit Ethernet ports 1 and 2 are NNIs and are enabled by default.

This is the overall sequence of initial configuration:

- Change the configured class map for an input service policy

- Change the configured class map for an output service policy

This example modifies classes for an input service policy by adding classification criteria to the silver-in class to also match dscp cs5. This is required for the output policy-map to match to dscp cs5:

```
Switch(config)# class-map match-any silver-in
Switch(config-cmap)# match ip dscp af21
Switch(config-cmap)# match ip dscp cs5
Switch(config-cmap)# exit
```

This example modifies classes for an output service policy, adding classification criteria to the silver-out class to also match dscp cs5. This adds dscp cs5 to the silver-out class on all configured and attached output service policies. The dscp cs5 flow now receives the same queuing and scheduling treatment as the silver-out class.

```
Switch# config terminal
Switch(config)# class-map match-any silver-out
Switch(config-cmap)# match ip dscp af21
Switch(config-cmap)# match ip dscp cs5
Switch(config-cmap)# exit
```

You should use the same procedure when deleting a match statement associated with a configured class.

Modifying Output Policies and Changing Queuing or Scheduling Parameters

This section provides examples of updating an existing set of output policy maps to modify the parameters of the configured queuing and scheduling actions. The modification in the output policy map might be required due to a change in the service provisioning requirements. You can make the change without shutting down any port.

In the initial configuration, Fast Ethernet ports 1 through 12 are UNIs and are active. Fast Ethernet ports 13 through 24 are UNIs and are shut down. Gigabit Ethernet ports 1 and 2 are NNIs and are enabled by default.

The requirement is to change the action parameters.

Output Policy Restrictions

Note these restrictions when configuring output policies:

- You can define up to three classes in the output policy map
- The defined classes must be the same as other output policy maps
- The number of defined classes in each output policy map must be same
- You must assign an action to each class; that is, there can be no empty class
- Each class configuration must be based on the classification or marking done in the input policy-map

This example modifies the third output service policy servicing Fast Ethernet UNIs 8 through 12 by providing minimum guaranteed bandwidth of 40 Mb/s to the gold class (changed from 50 Mb/s), 30 Mb/s to the silver class (changed from 20 Mb/s), and 20 Mb/s to the bronze class (changed from 10 Mbps).

```
Switch(config)# policy-map output9-12
Switch(config-pmap)# class gold-out
Switch(config-pmap-c)# bandwidth 40000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver-out
Switch(config-pmap-c)# bandwidth 30000
```

```
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze-out
Switch(config-pmap-c)# bandwidth 20000
Switch(config-pmap-c)# exit
```

Modifying Output Policies and Adding or Deleting Configured Actions

This section provides examples of updating an existing set of output policy maps to add or delete queuing and scheduling actions. The modification in the output policy map might be required due to a change in the service provisioning requirements. You can make the change without shutting down ports that are not configured with the output policy map to be modified. But you must shut down the ports that are configured with that output policy map. Customers not using this output policy map are not affected.

In the initial configuration, Fast Ethernet ports 1 through 12 are UNIs and are active. Fast Ethernet ports 13 through 24 are UNIs and are shut down. Gigabit Ethernet ports 1 and 2 are NNIs and are enabled by default.

This is the overall sequence of configuration:

- Shut down all active ports carrying the policy to be modified
- Detach the output policy from all ports to which it is attached
- Make modifications to the output policy
- Reattach the output policy to the appropriate ports
- Take the ports out of the shutdown state

Note these restrictions for configuring output policies:

- You can define up to three classes in the output policy map
- The defined classes must be the same as other output policy maps
- The number of defined classes in each output policy map must be same
- You must assign an action to each class; that is, there can be no empty class
- Each class configuration must be based on the classification/marking done in the input policy-map

These steps shut down all ports carrying the output policy, in this case only the Gigabit Ethernet ports

```
Switch(config)# interface range gigabitEthernet0/1-2
Switch(config-if-range)# shutdown
Switch(config-if-range)# exit
```

.These steps detach the output policy to be modified, in this case the one configured on the Gigabit Ethernet ports:

```
Switch(config)# interface range gigabitEthernet0/1-2
Switch(config-if-range)# no service-policy output output-g1-2
Switch(config-if-range)# exit
```

These steps modify the output service policy servicing the Gigabit Ethernet NNIs. Instead of providing a minimum bandwidth guarantee of 10 percent to the bronze class, the policy is modified to provide class-based shaping to 100000 bps.

```
Switch(config)# policy-map output-g1-2
Switch(config-pmap)# class bronze-out
Switch(config-pmap-c)# no bandwidth percent 10
Switch(config-pmap-c)# shape average 100000
Switch(config-pmap-c)# exit
```

These steps reattach the output policy to the Gigabit Ethernet ports:

```
Switch(config)# interface range gigabitethernet0/1-2
Switch(config-if-range)# service-policy output output9-12
Switch(config-if-range)# exit
```

These steps activate all Gigabit Ethernet ports:

```
Switch(config)# interface range gigabitethernet0/1-2
Switch(config-if-range)# no shutdown
Switch(config-if-range)# exit
```

Modifying Output Policies and Adding or Deleting a Class

This section provides examples of updating an existing set of output policy maps to add or delete entire classes. The modification in the output policy map might be required due to a change in the service provisioning requirements or a change in the input service policy. To make this change, you must shut down all active ports on the switch module. For this kind of update to any output policy map, all customers could potentially be affected. To avoid this, we recommend that you consider possible future upgrades when you configure classes in output service policies.

In the initial configuration, Fast Ethernet ports 1 through 12 are UNIs and are active. Fast Ethernet ports 13 through 24 are UNIs and are shut down. Gigabit Ethernet ports 1 and 2 are NNIs and are enabled by default.

This is the overall sequence of configuration:

- Shut down all active ports.
- Detach the output policies from all Fast Ethernet and Gigabit Ethernet ports.
- Delete the class.
- Reattach the output policies to the Fast Ethernet and Gigabit Ethernet ports.
- Take the Fast Ethernet and Gigabit Ethernet ports out of the shutdown state.

These steps shut down all active and applicable Fast Ethernet and Gigabit Ethernet ports:

```
Switch(config)# interface range gigabitethernet0/1-2, fastethernet0/1-12
Switch(config-if-range)# shutdown
Switch(config-if-range)# exit
```

These steps detach all output policies from the affected Fast Ethernet and Gigabit Ethernet ports:

```
Switch(config)# interface range fastethernet0/1-8
Switch(config-if-range)# no service-policy output output1-8
Switch(config-if-range)# exit

Switch(config)# interface range fastethernet0/9-12
Switch(config-if-range)# no service-policy output output9-12
Switch(config-if-range)# exit

Switch(config)# interface range gigabitethernet0/1/0-2
Switch(config-if-range)# no service-policy output output-g1-2
Switch(config-if-range)# exit
```

These steps delete a class from all output policy maps and input policy maps; the input policy can be left attached or can be detached:

```
Switch(config)# policy-map output1-8
Switch(config-pmap)# no class bronze-out
Switch(config-pmap-c)# exit
Switch(config)# policy-map output9-12
Switch(config-pmap)# no class bronze-out
Switch(config-pmap-c)# exit
Switch(config)# policy-map output-g1-2
Switch(config-pmap)# no class bronze-out
Switch(config-pmap-c)# exit
Switch(config)# policy-map input-all
Switch(config-pmap)# no class bronze-in
Switch(config-pmap-c)# exit
```

These steps reattach all policies to the Fast Ethernet and Gigabit Ethernet ports:

```
Switch(config)# interface range fastethernet0/1-8
Switch(config-if-range)# service-policy output output1-8
Switch(config-if-range)# exit

Switch(config)# interface range fastethernet0/9-12
Switch(config-if-range)# service-policy output output9-12
Switch(config-if-range)# exit

Switch(config)# interface range gigabitethernet0/1/0-2
Switch(config-if-range)# service-policy output output9-12
Switch(config-if-range)# exit
```

These steps activate all applicable Fast Ethernet and Gigabit Ethernet ports:

```
Switch(config)# interface range gigabitethernet0/1-2, fastethernet0/1-12
Switch(config-if-range)# no shutdown
Switch(config-if-range)# exit
```

You should use the same procedure when adding a class to an attached output service policy.

Note Problems can occur if you do not follow the previous sequence.

When a policy map is attached to an interface, all traffic that does not explicitly match the configured class maps within the policy map should go through the default queue (class **class-default**). However, in some cases, traffic that does not explicitly match the output policy-map classes could go through more than one queue. This queuing problem can occur when you do not follow the previous procedure and do not attach an output policy to all active ports.

For example, consider this case where only two ports are configured with an output policy and we want to delete a class in the output policy.

Shut down two ports:

```
Switch(config)# interface range fastethernet0/1-2
Switch(config-if-range)# shutdown
Switch(config-if-range)# exit
```

Detach the output policy from both ports:

```
Switch(config)# interface range fastEthernet0/1-2
Switch(config-if)# no service-policy output output1-2
Switch(config-if)# exit
```

Delete a class in the output policy:

```
Switch(config)# policy-map output1-2
```

```
Switch(config-pmap)# no class bronze-out
Switch(config-pmap-c)# exit
```

Attach the output policy to only one port and not to the other:

```
Switch(config)# interface FastEthernet0/1
Switch(config-if)# service-policy output output1-2
Switch(config-if)# exit
```

Enable both ports:

```
Switch(config)# interface range fastethernet0/1-2
Switch(config-if-range)# no shutdown
Switch(config-if-range)# exit
```

At this point, when traffic leaves Fast Ethernet port 2, instead of going through a single default-queue, it goes through the same number of queues as there are classes defined in the output policy-map attached to Fast Ethernet port 1. In this case, it would be three queues. In some cases, packets for a flow out of Fast Ethernet port 2 might be reordered if a flow splits across more than one queue. You can avoid this problem by leaving ports in a shut-down state until you attach an output policy.

Implementing High-Priority Traffic to the Host Router

This section describes QoS features for implementing high-priority (low-latency) traffic via the internal data path between the CGR 2010 ESM and the host CGR 2010 router. The internal data path is called *PortChannel48*. For details, see Chapter 9, "EtherChannel Configuration Between the Switch Module and the Host Router."

Note In this section, *ingress* refers to the direction of the data flow from the CGR 2010 ESM to the host router and *egress* refers to the direction of the data flow from the host router to the switch module.

Tip QoS configuration for the switch module is concerned only with the ingress traffic from the switch module to the host router.

You can configure QoS on the switch module and the CGR 2010 router using Modular QoS CLI (MQC), with some limitations on the switch module. The following subsections describe the major components in this internal data path and their QoS functions.

Ingress CoS to GDF Queue Mapping

In a substation network, some data frames (for example, GOOSE (Generic Object Oriented Substation Events) messages) require low-latency in the data path. The switch module provides high priority queuing to support low-latency data. This section describes how low-latency data frames from the switch module are mapped to the Generic Data Frame (GDF) queues.

Unlike the switch module, which uses a hardware ASIC to perform Layer 2 to Layer 3 switching, the CGR 2010 router's data path is implemented in software and can potentially have greater jitter and delay in its data path. If all data packets from the switch module are sent to a single GDF queue in the CGR 2010 router, low-latency data could be blocked by the other low priority data frames in the same queue.

To prevent low-latency data frames from being blocked by other lower priority data frames on the ingress data path to the host CGR 2010 router, the switch module sends high priority data frames and the other lower priority data frames to two separate GDF queues:

- The GDF queue for low-latency (high-priority) data is called the *priority queue* (GDF queue 0).
- The GDF queue for other data is called the *low-priority queue* (GDF queue 1).

Network administrators can use MQC to classify and/or mark a data frame based on the information on the Layer 2 and Layer 3 headers. *The mapping of data frames to GDF queues is solely based on the CoS field in the 802.1Q tag.* Data frames that require low latency in the internal data path from the switch module to the host router should contain an 802.1Q tag and be marked with CoS values that are configured with priority queuing (with or without policing).

All other data frames, which either do not contain an 802.1Q tag or their CoS values are not configured with priority queuing, are mapped to the low-priority queue. For details and example configurations, see "Mapping CoS to the High-Priority GDF Queue" section on page 14-97.

Adjusting for Differences in Ingress Traffic Bandwidth

The CGR 2010 router processes incoming and outgoing packets in software. Depending on the performance of the router's CPU, the effective bandwidth of the internal data path on the CGR 2010 router's side could be less than the bandwidth provided by the internal EtherChannel on the switch module.

If the effective bandwidth on the CGR 2010 router is less than the bandwidth of the internal EtherChannel, you should use the **MQC** command to configure port shaping on the internal EtherChannel on the switch module so that the effective bandwidth on the two sides are roughly equivalent. For more information, see the "Congestion Management and Scheduling" section on page 14-26.

Configuring CPU-Generated Data

The switch module can send control data to the CGR 2010 host router through the backplane PortChannel48. You can configure QoS for the CPU-generated data frames with MQC. If you would like to send the CPU-generated data frames to the GDF priority queue, you have to configure the CPU so that all CPU-generated data would be marked with a non-zero CoS value.

To do so, use the **cpu traffic qos cos** command in global configuration mode to configure quality of service (QoS) marking based on class of service (CoS) for control plane traffic. To return to the default value, use the **no** form of this command.

cpu traffic qos cos {*cos_value* }

For example:

```
Switch(config)# cpu traffic qos cos 5
```

Syntax	Description
cos-value	Specify a CoS value. The range is from 0 to 7. If no CoS value is configured, the protocol-specific default value for each packet is applied.
cos	Configure the CoS value based on the CoS value in the packet, using a table-map.

Usage Guidelines

Configure any desired table-maps before configuring marking or queuing of CPU traffic.

This feature must be configured globally for a switch module; it cannot be configured per-port or per-protocol.

Enter each cpu traffic qos marking action on a separate line.

The **cpu traffic qos cos** global configuration command configures CoS marking for CPU-generated traffic by using either a specific CoS value or a table map, but not both. A new configuration overwrites the existing configuration.

When the **cpu traffic qos cos** global configuration command is configured with table maps, you can configure two **map from** values at a time—*CoS* and either *DSCP* or *precedence*.

Mapping CoS to the High-Priority GDF Queue

As mentioned earlier in this section, GDF queue mapping is solely based on the CoS value in the 802.1Q tag. Untagged data frames are mapped to the GDF low-priority queue. This imposes some limitations on how users configure QoS on the internal PortChannel interface in the CGR 2010 ESM.

A *native VLAN* is the untagged VLAN on an 802.1Q trunked switch module port. The native VLAN and management VLAN could be the same, but it is better security practice that they are not. If a switch module receives untagged frames on a trunk port, they are assumed to be part of the VLAN that is designated on the switch module port as the native VLAN. Frames egressing a switch module port on the native VLAN are not tagged.

By default, the data frames belonging to a native VLAN are untagged. If users would like to configure priority queuing for native VLAN, they should use the **vlan dot1q tag native** CLI command to enable 802.1Q tagging for native VLAN.

Note **vlan dot1q tag native** is a global configuration command and applies to all trunk ports in the switch module.

Please note the following:

- Users should not configure priority queuing for data frames marked with CoS 0 because it is the default CoS value for data frames whose CoS value are not marked.
- Low-latency traffic destined to the GDF priority queue should be marked with a non-zero CoS value and configured with priority queuing using MQC (see the "Modular QoS CLI" section on page 14-3).
- Chosen CoS values for priority queuing applies to the data frame for all VLANs

Example Configuration for CoS to GDF Queue Mapping

This section provides an example configuration to map CoS 5 to GDF queue 0 (the high-priority queue) for the internal PortChannel 48 on the CGR 2010 ESM copper model (GRWIC-D-2S-8PC).

	Step	Command
Step 1	Enters global configuration mode.	**configure terminal**
Step 2	Creates a class map, and enters class-map configuration mode. For details on using the **class-map** command, see the "Using Class Maps to Define a Traffic Class" section on page 14-42. • In this example, we use the **match-all** keyword to perform a logical-AND of all matching statements under this class map. All match criteria in the class map must be matched. • In this example, *class0* specifies the name of the class map.	**class-map match-all class0**
Step 3	Defines the match criterion to classify traffic. Only one match type per class map is supported, and only one ACL per class map is supported. • The **cos 5** parameter specifies a value of **5** for the CoS field to match against incoming packets.	**match cos 5**
Step 4	Creates a policy map by entering the policy map name (for example, *policy0*), and enters policy-map configuration mode.	**policy-map policy0**
Step 5	Enters the name of the priority class (created by using the **class-map** global configuration command shown in Step 2), and enters policy-map class configuration mode for the priority class.	**class class0**
Step 6	Sets the strict scheduling priority for this class.	**priority**
Step 7	Specifies the interface to configure, and enters interface configuration mode.	**interface FastEthernet0/9**
Step 8	Configures the switch's PortChannel as a Layer 2 VLAN trunk, so that the specified port can transport the frames for multiple VLANs.	**switchport mode trunk**
Step 9	The **service-policy output policy0** interface configuration command attaches all the characteristics of the traffic policy named **policy0** to the specified interface. All packets leaving the specified interface are evaluated according to the criteria specified in the traffic policy named **policy0**.	**service-policy output policy0**

	Step	Command
Step 10	Repeat Steps 7 through 9 for each interface in the PortChannel48 (a total of eight interfaces).	
Step 11	Return to privileged EXEC mode.	**end**
Step 12	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

EtherChannel Configuration and Link State Tracking

This chapter describes how to configure EtherChannels on Layer 2 and Layer 3 ports on the CGR 2010 ESM. EtherChannel provides fault-tolerant high-speed links between switches, routers, and servers. You can use it to increase the bandwidth between the wiring closets and the data center, and you can deploy it anywhere in the network where bottlenecks are likely to occur.

EtherChannel provides automatic recovery for the loss of a link by redistributing the load across the remaining links. If a link fails, EtherChannel redirects traffic from the failed link to the remaining links in the channel without intervention. This chapter also describes how to configure link-state tracking.

For information about configuring the backplane PortChannel48 interface, which provides communication between the host router and the switch module, see Chapter 9, "EtherChannel Configuration Between the Switch Module and the Host Router."

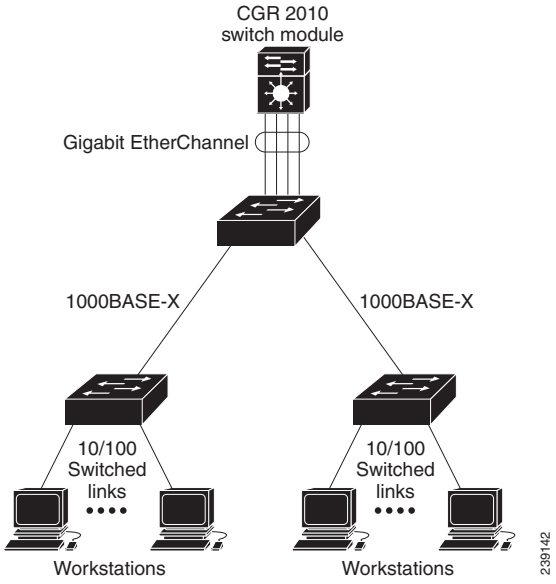
Note For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

Understanding EtherChannels

EtherChannel Overview

An EtherChannel consists of individual Fast Ethernet or Gigabit Ethernet links bundled into a single logical link as shown in Figure 15-1.

Figure 15-1 Typical EtherChannel Configuration



The EtherChannel provides full-duplex bandwidth of up to 800 Mbps between your switch module and another switch module or host for Fast EtherChannel on a switch module with 24 Fast Ethernet ports. For Gigabit EtherChannel, you can configure up to 8 Gbps (8 ports of 1 Gbps), depending on the number of supported Gigabit Ethernet interfaces.

Note Only network node interfaces (NNIs) and enhanced network interfaces (ENIs) support Link Aggregation Control Protocol (LACP). Use the **port-type** {**eni** | **nni**} interface configuration command to configure a port as an ENI or NNI. The switch module must be running the IP services image to allow configuring of more than four ports as NNIs.

Each EtherChannel can consist of up to eight compatibly configured Ethernet ports. All ports in each EtherChannel must be configured as either Layer 2 or Layer 3 ports. The number of EtherChannels is limited to 48. For more information, see the "EtherChannel Configuration Guidelines" section on page 15-8. The EtherChannel Layer 3 ports are made up of routed ports. Routed ports are physical ports configured to be in Layer 3 mode by using the **no switchport** interface configuration command. For more information, see Chapter 8, "Interface Configuration."

You can configure an EtherChannel in one of these modes: Link Aggregation Control Protocol (LACP) or On mode. LACP is available only on NNIs and ENIs. Configure both ends of the EtherChannel in the same mode:

- When you configure one end of an EtherChannel inr LACP mode, the system negotiates with the other end of the channel to determine which ports should become active. Incompatible ports are suspended.

- When you configure an EtherChannel in the **on** mode, no negotiations take place. The switch module forces all compatible ports to become active in the EtherChannel. The other end of the channel (on the other switch module) must also be configured in the **on** mode; otherwise, packet loss can occur.

  The local port is put into an independent state and continues to carry data traffic as would any other single link. The port configuration does not change, but the port does not participate in the EtherChannel.

If a link within an EtherChannel fails, traffic previously carried over that failed link changes to the remaining links within the EtherChannel. A trap is sent for a failure, identifying the switch module, the EtherChannel, and the failed link. Inbound broadcast and multicast packets on one link in an EtherChannel are blocked from returning on any other link of the EtherChannel.

Port-Channel Interfaces

When you create an EtherChannel, a port-channel logical interface is involved:

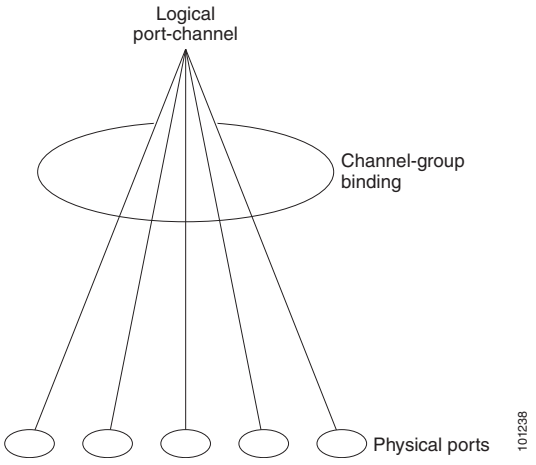
- With Layer 2 ports, use the **channel-group** interface configuration command to dynamically create the port-channel logical interface.

  You also can use the **interface port-channel** *port-channel-number* global configuration command to manually create the port-channel logical interface, but then you must use the **channel-group** *channel-group-number* command to bind the logical interface to a physical port. The *channel-group-number* can be the same as the *port-channel-number,* or you can use a new number. If you use a new number, the **channel-group** command dynamically creates a new port channel.
- With Layer 3 ports, you should manually create the logical interface by using the **interface port-channel** global configuration command followed by the **no switchport** interface configuration command. Then you manually assign an interface to the EtherChannel by using the **channel-group** interface configuration command.

For both Layer 2 and Layer 3 ports, the **channel-group** command binds the physical port and the logical interface together as shown in Figure 15-2.

Each EtherChannel has a port-channel logical interface numbered from 1 to 48. This port-channel interface number corresponds to the one specified with the **channel-group** interface configuration command.

Figure 15-2 Relationship of Physical Ports, Logical Port Channels, and Channel Groups



After you configure an EtherChannel, configuration changes applied to the port-channel interface apply to all the physical ports assigned to the port-channel interface. Configuration changes applied to the physical port affect only the port to which you apply the configuration. To change the parameters of all ports in an EtherChannel, apply the configuration commands to the port-channel interface.

Link Aggregation Control Protocol

The LACP is defined in IEEE 802.3ad standard and enables Cisco switches to manage Ethernet channels between switches that conform to the standard. LACP facilitates the automatic creation of EtherChannels by exchanging LACP packets between Ethernet ports.

Note LACP is available only on NNIs and ENIs.

By using LACP, the switch module learns the identity of partners capable of supporting LACP and the capabilities of each port. It then dynamically groups similarly configured ports into a single logical link (channel or aggregate port). Similarly configured ports are grouped based on hardware, administrative, and port parameter constraints. For example, LACP groups the ports with the same speed, duplex mode, native VLAN, VLAN range, and trunking status and type. After grouping the links into an EtherChannel, LACP adds the group to the spanning tree as a single switch module port.

LACP Modes

Table 15-1 shows the user-configurable EtherChannel LACP modes for the **channel-group** interface configuration command on an NNI or ENI.

Table 15-1 EtherChannel LACP Modes

Mode	Description
active	Places a port into an active negotiating state in which the port starts negotiations with other ports by sending LACP packets.
passive	Places a port into a passive negotiating state in which the port responds to LACP packets that it receives, but does not start LACP packet negotiation. This setting minimizes the transmission of LACP packets.

Both the **active** and **passive LACP** modes enable ports to negotiate with partner ports to an EtherChannel based on criteria such as port speed and, for Layer 2 EtherChannels, trunking state and VLAN numbers.

Ports can form an EtherChannel when they are in different LACP modes as long as the modes are compatible. For example:

- A port in the **active** mode can form an EtherChannel with another port that is in the **active** or **passive** mode.
- A port in the **passive** mode cannot form an EtherChannel with another port that is also in the **passive** mode because neither port starts LACP negotiation.

LACP Interaction with Other Features

The CDP sends and receives packets over the physical ports in the EtherChannel. Trunk ports send and receive LACP PDUs on the lowest numbered VLAN.

In Layer 2 EtherChannels, the first port in the channel that comes up provides its MAC address to the EtherChannel. If this port is removed from the bundle, one of the remaining ports in the bundle provides its MAC address to the EtherChannel.

LACP sends and receives LACP PDUs only from ports that are up and have LACP enabled for the active or passive mode.

EtherChannel On Mode

EtherChannel **on** mode can be used to manually configure an EtherChannel. The **on** mode forces a port to join an EtherChannel without negotiations. It can be useful if the remote device does not support LACP. With the **on** mode, a usable EtherChannel exists only when both ends of the link are configured in the **on** mode.

Note For UNIs, the only available mode is **on**.

Ports that are configured in the **on** mode in the same channel group must have compatible port characteristics, such as speed and duplex. Ports that are not compatible are suspended, even though they are configured in the **on** mode.

Caution You should use care when using the **on** mode. This is a manual configuration, and ports on both ends of the EtherChannel must have the same configuration. If the group is misconfigured, packet loss or spanning-tree loops can occur.

Load Balancing and Forwarding Methods

EtherChannel balances the traffic load across the links in a channel by reducing part of the binary pattern formed from the addresses in the frame to a numerical value that selects one of the links in the channel. EtherChannel load balancing can use MAC addresses or IP addresses, source or destination addresses, or both source and destination addresses. The selected mode applies to all EtherChannels configured on the switch module. You configure the load balancing and forwarding method by using the **port-channel load-balance** global configuration command.

With source-MAC address forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the channel based on the source-MAC address of the incoming packet. To provide load balancing, packets from different hosts use different ports in the channel, but packets from the same host use the same port in the channel.

With destination-MAC address forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the channel based on the destination-host MAC address of the incoming packet. Packets to the same destination are forwarded over the same port, and packets to a different destination are sent on a different port in the channel.

On the CGR 2010 ESM, load distribution based on the destination host MAC address supports only four ports per EtherChannel. When you configure EtherChannel destination-MAC address load balancing, the traffic is balanced only among four ports in the channel group.If you configure more than four ports in an EtherChannel with destination host MAC address load distribution, only four of the ports receive distributed traffic. This limitation does not apply to the other load distribution methods.

With source-and-destination MAC address forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the channel based on both the source and destination MAC addresses. This forwarding method, a combination source-MAC and destination-MAC address forwarding methods of load distribution, can be used if it is not clear whether source-MAC or destination-MAC address forwarding is better suited on a particular switch module. With source-and-destination MAC-address forwarding, packets sent from host A to host B, host A to host C, and host C to host B could all use different ports in the channel.

With source-IP-address-based forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the EtherChannel based on the source-IP address of the incoming packet. To provide load-balancing, packets from different IP addresses use different ports in the channel, but packets from the same IP address use the same port in the channel.

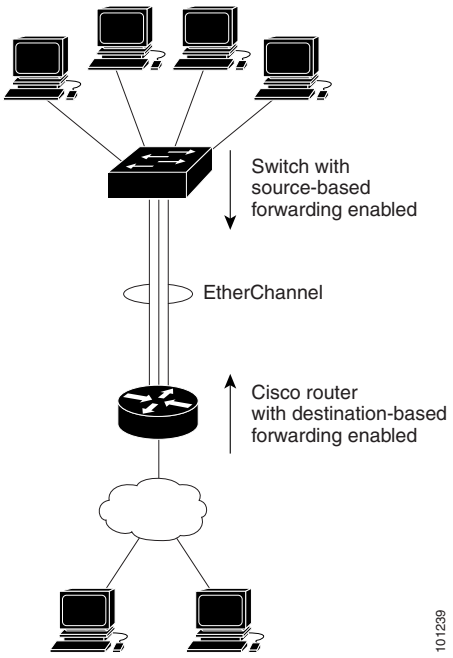
With destination-IP-address-based forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the EtherChannel based on the destination-IP address of the incoming packet. To provide load-balancing, packets from the same IP source address sent to different IP destination addresses could be sent on different ports in the channel. But packets sent from different source IP addresses to the same destination IP address are always sent on the same port in the channel.

With source-and-destination IP address-based forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the EtherChannel based on both the source and destination IP addresses of the incoming packet. This forwarding method, a combination of source-IP and destination-IP address-based forwarding, can be used if it is not clear whether source-IP or destination-IP address-based forwarding is better suited on a particular switch module. In this method, packets sent from the IP address A to IP address B, from IP address A to IP address C, and from IP address C to IP address B could all use different ports in the channel.

Different load-balancing methods have different advantages, and the choice of a particular load-balancing method should be based on the position of the switch module in the network and the kind of traffic that needs to be load-distributed. In Figure 15-3, an EtherChannel of four workstations communicates with a router. Because the router is a single-MAC-address device, source-based forwarding on the switch module EtherChannel ensures that the switch module uses all available bandwidth to the router. The router is configured for destination-based forwarding because the large number of workstations ensures that the traffic is evenly distributed from the router EtherChannel.

Use the option that provides the greatest variety in your configuration. For example, if the traffic on a channel is going only to a single MAC address, using the destination-MAC address always chooses the same link in the channel. Using source addresses or IP addresses might result in better load balancing.

Figure 15-3 Load Distribution and Forwarding Methods



Configuring EtherChannels

Note Make sure that the ports are correctly configured. For more information, see the "EtherChannel Configuration Guidelines" section on page 15-8.

Note After you configure an EtherChannel, configuration changes applied to the port-channel interface apply to all the physical ports assigned to the port-channel interface, and configuration changes applied to the physical port affect only the port to which you apply the configuration.

Default EtherChannel Configuration

Table 15-2 shows the default EtherChannel configuration.

Table 15-2 Default EtherChannel Configuration

Feature	Default Setting
Channel groups	None assigned.
Port-channel logical interface	None defined.
LACP mode	No default.
LACP learn method	Aggregate-port learning on all NNIs and ENIs.
LACP port priority	32768 on all NNIs and ENIs.
LACP system priority	32768.
LACP system ID	LACP system priority and the switch module MAC address.
Load balancing	Load distribution on the switch module is based on the source-MAC address of the incoming packet.

EtherChannel Configuration Guidelines

If improperly configured, some EtherChannel ports are automatically disabled to avoid network loops and other problems. Follow these guidelines to avoid configuration problems:

- Do not try to configure more than 48 EtherChannels on the switch module.
- Configure a LACP EtherChannel including only NNIs or only ENIs.
- Configure all ports in an EtherChannel to operate at the same speeds and duplex modes.
- All ports in an EtherChannel must be the same type, either UNI, NNI, or ENI. You cannot mix port types in an EtherChannel.
- On UNIs, the EtherChannel mode must always be configured to **on**.
- Enable all ports in an EtherChannel. A port in an EtherChannel that is disabled by using the **shutdown** interface configuration command is treated as a link failure, and its traffic is transferred to one of the remaining ports in the EtherChannel. UNIs and ENIs are disabled by default. NNIs are enabled by default.
- When a group is first created, all ports follow the parameters set for the first port to be added to the group. If you change the configuration of one of these parameters, you must also make the changes to all ports in the group:
  - Allowed-VLAN list
  - Spanning-tree path cost for each VLAN
  - Spanning-tree port priority for each VLAN
  - Spanning-tree Port Fast setting

  Note Spanning Tree Protocol is only supported on NNIs or ENIs on which it has been specifically enabled.

- Do not configure a port to be a member of more than one EtherChannel group.

- Do not configure an EtherChannel in LACP mode. EtherChannel groups running LACP can coexist on the same switch module. Individual EtherChannel groups can run LACP, but they cannot interoperate.

Note LACP is only available on NNIs and ENIs.

- If the switch module is running the CGR 2010 LAN base image, you can have only four NNIs on the switch module at the same time; only four ports in an EtherChannel can support LACP at the same time.If the switch module is running the IP services image, there is no limit to the number of NNIs that can be configured on the switch module.
- Do not configure a Switched Port Analyzer (SPAN) destination port as part of an EtherChannel.
- Do not configure a secure port as part of an EtherChannel or the reverse.
- Do not configure a private-VLAN port as part of an EtherChannel.
- Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an 802.1x port. If you try to enable 802.1x on an EtherChannel port, an error message appears, and 802.1x is not enabled.
- If EtherChannels are configured on switch module interfaces, remove the EtherChannel configuration from the interfaces before globally enabling 802.1x on a switch module by using the **dot1x system-auth-control** global configuration command.
- Do not enable link-state tracking on individual interfaces that will be part of a downstream Etherchannel interface.
- For Layer 2 EtherChannels:
  - Assign all ports in the EtherChannel to the same VLAN, or configure them as trunks. Ports with different native VLANs cannot form an EtherChannel.
  - If you configure an EtherChannel from trunk ports, verify that the trunking mode is the same on all the trunks. Inconsistent trunk modes on EtherChannel ports can have unexpected results.
  - An EtherChannel supports the same allowed range of VLANs on all the ports in a trunking Layer 2 EtherChannel.
  - NNIs or ENIs with different spanning-tree path costs can form an EtherChannel if they are otherwise compatibly configured. Setting different spanning-tree path costs does not, by itself, make ports incompatible for the formation of an EtherChannel.
- For Layer 3 EtherChannels, assign the Layer 3 address to the port-channel logical interface, not to the physical ports in the channel.

Configuring Layer 2 EtherChannels

You configure Layer 2 EtherChannels by assigning ports to a channel group with the **channel-group** interface configuration command. This command automatically creates the port-channel logical interface.

Beginning in privileged EXEC mode, follow these steps to assign a Layer 2 Ethernet port to a Layer 2 EtherChannel. This procedure is required.

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify a physical port, and enter interface configuration mode. Valid interfaces include physical ports. For a LACP EtherChannel, you can configure up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode. **Note** If the interface is a UNI, you must enter the **port-type** {**eni** | **nni**} interface configuration command before configuring LACP.	**interface** *interface-id*
Step 3	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.	**no shutdown**
Step 4	Assign all ports as static-access ports in the same VLAN, or configure them as trunks. If you configure the port as a static-access port, assign it to only one VLAN. The range is 1 to 4094.	**switchport mode** {**access** | **trunk**} **switchport access vlan** *vlan-id*
Step 5	Assign the port to a channel group, and specify the LACP mode. For *channel-group-number*, the range is 1 to 48. **Note** For UNIs, the only available mode is **on**. For **mode**, select one of these keywords: • **on**—Forces the port to channel without LACP. With the **on** mode, a usable EtherChannel exists only when a port group in the **on** mode is connected to another port group in the **on** mode. • **active**—Enables LACP only if a LACP device is detected. It places the port into an active negotiating state in which the port starts negotiations with other ports by sending LACP packets. • **passive**—Enables LACP on the port and places it into a passive negotiating state in which the port responds to LACP packets that it receives, but does not start LACP packet negotiation.	**channel-group** *channel-group-number* **mode** {**auto** [**non-silent**] | **desirable** [**non-silent**] | **on**} | {**active** | **passive**}
Step 6	Return to privileged EXEC mode.	**end**

	Step	Command
Step 7	Verify your entries.	**show running-config**
Step 8	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To remove a port from the EtherChannel group, use the **no channel-group** interface configuration command.

This example shows how to configure an EtherChannel. It assigns two ports as static-access ports in VLAN 10 to channel 5 with the LACP mode **active**:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

Configuring Layer 3 EtherChannels

To configure Layer 3 EtherChannels, you create the port-channel logical interface and then put the Ethernet ports into the port-channel as described in the next two sections.

Creating Port-Channel Logical Interfaces

When configuring Layer 3 EtherChannels, you should first manually create the port-channel logical interface by using the **interface port-channel** global configuration command. Then you put the logical interface into the channel group by using the **channel-group** interface configuration command.

Note To move an IP address from a physical port to an EtherChannel, you must delete the IP address from the physical port before configuring it on the port-channel interface.

Beginning in privileged EXEC mode, follow these steps to create a port-channel interface for a Layer 3 EtherChannel. This procedure is required.

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the port-channel logical interface, and enter interface configuration mode. For *port-channel-number*, the range is 1 to 48.	**interface port-channel** *port-channel-number*
Step 3	Put the port-channel interface into Layer 3 mode.	**no switchport**
Step 4	Assign an IP address and subnet mask to the EtherChannel.	**ip address** *ip-address mask*
Step 5	Return to privileged EXEC mode.	**end**

	Step	Command
Step 6	Verify your entries.	**show etherchannel** *channel-group-number* **detail**
Step 7	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**
Step 8	Assign an Ethernet port to the Layer 3 EtherChannel. For more information, see the "Configuring the Physical Interfaces" section on page 15-12.	

To remove the port-channel, use the **no interface port-channel** *port-channel-number* global configuration command.

This example shows how to create the logical port channel 5 and assign 172.10.20.10 as its IP address:

```
Switch# configure terminal
Switch(config)# interface port-channel 5
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.10.20.10 255.255.255.0
Switch(config-if)# end
```

Configuring the Physical Interfaces

Beginning in privileged EXEC mode, follow these steps to assign an Ethernet port to a Layer 3 EtherChannel. This procedure is required.

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify a physical port, and enter interface configuration mode. Valid interfaces include physical ports. For a LACP EtherChannel, you can configure up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode. **Note** If the interface is a UNI, you must enter the **port-type** {**eni** | **nni**} interface configuration command before configuring LACP.	**interface** *interface-id*
Step 3	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.	**no shutdown**
Step 4	Ensure that there is no IP address assigned to the physical port.	**no ip address**
Step 5	Put the port into Layer 3 mode.	**no switchport**

	Step	Command
Step 6	Assign the port to a channel group, and specify the LACP mode. For *channel-group-number*, the range is 1 to 48. This number must be the same as the *port-channel-number* (logical port) configured in the "Creating Port-Channel Logical Interfaces" section on page 15-11. **Note** For UNIs, the only available mode is **on**. For **mode**, select one of these keywords: • **on**—Forces the port to channel without LACP. With the **on** mode, a usable EtherChannel exists only when a port group in the **on** mode is connected to another port group in the **on** mode. • **active**—Enables LACP only if a LACP device is detected. It places the port into an active negotiating state in which the port starts negotiations with other ports by sending LACP packets. • **passive**—Enables LACP on the port and places it into a passive negotiating state in which the port responds to LACP packets that it receives, but does not start LACP packet negotiation. For information on compatible modes for the switch and its partner, see the"LACP Modes" section on page 15-4.	**channel-group** *channel-group-number* **mode** {**auto** [**non-silent**] | **desirable** [**non-silent**] | **on**} | {**active** | **passive**}
Step 7	Return to privileged EXEC mode.	**end**
Step 8	Verify your entries.	**show running-config**
Step 9	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

This example shows how to configure an EtherChannel. It assigns two ports to channel 5 with the LACP mode **active**:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 -2
Switch(config-if-range)# no ip address
Switch(config-if-range)# no switchport
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

Configuring EtherChannel Load Balancing

This section describes how to configure EtherChannel load balancing by using source-based or destination-based forwarding methods. For more information, see the "Load Balancing and Forwarding Methods" section on page 15-5.

Beginning in privileged EXEC mode, follow these steps to configure EtherChannel load balancing. This procedure is optional.

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Configure an EtherChannel load-balancing method. The default is **src-mac**. Select one of these load-distribution methods: • **dst-ip**—Load distribution is based on the destination-host IP address. • **dst-mac**—Load distribution is based on the destination-host MAC address of the incoming packet. **Note** When you enter the **dst-mac** keyword, the traffic is balanced only among four ports in the channel group. If you configure more than four ports in an EtherChannel with destination host MAC address load distribution, only four of the ports receive distributed traffic.This limitation does not apply to the other load distribution methods. • **src-dst-ip**—Load distribution is based on the source-and-destination host-IP address. • **src-dst-mac**—Load distribution is based on the source-and-destination host-MAC address. • **src-ip**—Load distribution is based on the source-host IP address. • **src-mac**—Load distribution is based on the source-MAC address of the incoming packet.	**port-channel load-balance** {**dst-ip** | **dst-mac** | **src-dst-ip** | **src-dst-mac** | **src-ip** | **src-mac**}
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entries.	**show etherchannel load-balance**
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To return EtherChannel load balancing to the default configuration, use the **no port-channel load-balance** global configuration command.

Configuring LACP Hot-Standby Ports

When enabled, LACP tries to configure the maximum number of LACP-compatible ports in a channel, up to a maximum of 16 ports. Only eight LACP links can be active at one time. The software places any additional links in a hot-standby mode. If one of the active links becomes inactive, a link that is in the hot-standby mode becomes active in its place.

Note LACP is only available on NNIs and ENIs.

If you configure more than eight links for an EtherChannel group, the software automatically decides which of the hot-standby ports to make active based on the LACP priority. The software assigns to every link between systems that operate LACP a unique priority made up of these elements (in priority order):

- LACP system priority
- System ID (a combination of the LACP system priority and the switch module MAC address)
- LACP port priority
- Port number

In priority comparisons, numerically lower values have higher priority. The priority decides which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

Ports are considered for active use in aggregation in link-priority order starting with the port attached to the highest priority link. Each port is selected for active use if the preceding higher priority selections can also be maintained. Otherwise, the port is selected for standby mode.

You can change the default values of the LACP system priority and the LACP port priority to affect how the software selects active and standby links. For more information, see the "Configuring the LACP System Priority" section on page 15-15 and the "Configuring the LACP Port Priority" section on page 15-16.

Configuring the LACP System Priority

You can configure the system priority for all of the EtherChannels that are enabled for LACP by using the **lacp system-priority** global configuration command. You cannot configure a system priority for each LACP-configured channel. By changing this value from the default, you can affect how the software selects active and standby links.

You can use the **show etherchannel summary** privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag).

Beginning in privileged EXEC mode, follow these steps to configure the LACP system priority. This procedure is optional.

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Configure the LACP system priority. For *priority*, the range is 1 to 65535. The default is 32768. The lower the value, the higher the system priority.	**lacp system-priority** *priority*

	Step	Command
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Verify your entries.	**show running-config** or **show lacp sys-id**
Step 5	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To return the LACP system priority to the default value, use the **no lacp system-priority** global configuration command.

Configuring the LACP Port Priority

By default, all ports use the same port priority. If the local system has a lower value for the system priority and the system ID than the remote system, you can affect which of the hot-standby links become active first by changing the port priority of LACP EtherChannel ports to a lower value than the default. The hot-standby ports that have lower port numbers become active in the channel first. You can use the **show etherchannel summary** privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag).

Note If LACP is not able to aggregate all the ports that are compatible (for example, the remote system might have more restrictive hardware limitations), all the ports that cannot be actively included in the EtherChannel are put in the hot-standby state and are used only if one of the channeled ports fails.

Beginning in privileged EXEC mode, follow these steps to configure the LACP port priority. This procedure is optional.

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the port to be configured, and enter interface configuration mode. **Note** If the interface is a UNI, you must enter the **port-type** {**eni** | **nni**} interface configuration command before configuring LACP.	**interface** *interface-id*
Step 3	Configure the LACP port priority. For *priority*, the range is 1 to 65535. The default is 32768. The lower the value, the more likely that the port will be used for LACP transmission.	**lacp port-priority** ***priority***
Step 4	Return to privileged EXEC mode.	**end**

	Step	Command
Step 5	Verify your entries.	**show running-config** or **show lacp** [*channel-group-number*] **internal**
Step 6	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To return the LACP port priority to the default value, use the **no lacp port-priority** interface configuration command.

Displaying EtherChannel and LACP Status

To display EtherChannel and LACP status information, use the privileged EXEC commands described in Table 15-3:

Table 15-3 Commands for Displaying EtherChannel and LACP Status

Command	Description
show etherchannel [*channel-group-number* {**detail** | **port** | **port-channel** | **protocol** | **summary**}] {**detail** | **load-balance** | **port** | **port-channel** | **protocol** | **summary**}	Displays EtherChannel information in a brief, detailed, and one-line summary form. Also displays the load-balance or frame-distribution scheme, port, port-channel, and protocol information.
show lacp [*channel-group-number*] {**counters** | **internal** | **neighbor**}	Displays LACP information such as traffic information, the internal LACP configuration, and neighbor information.

You can clear LACP channel-group information and traffic counters by using the **clear lacp** {*channel-group-number* **counters** | **counters**} privileged EXEC command.

For detailed information about the fields in the displays, see the command reference for this release.

Understanding Link-State Tracking

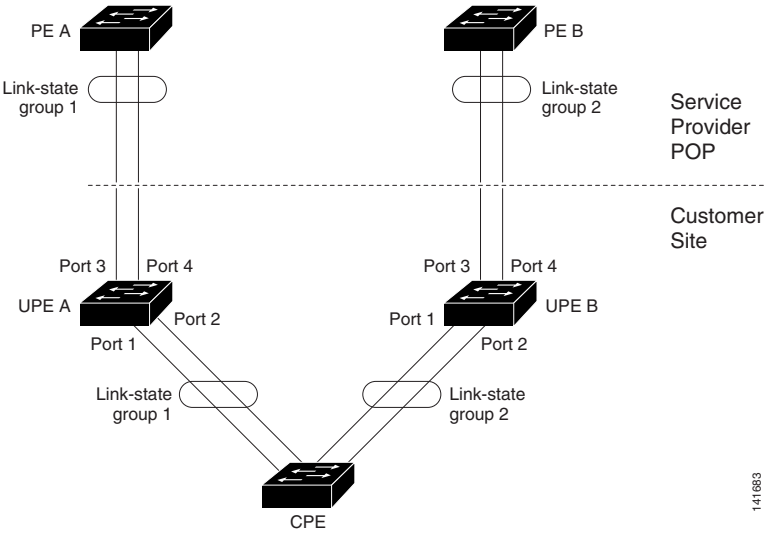
Link-state tracking, also known as trunk failover, is a feature that binds the link state of multiple interfaces. For example, link-state tracking provides redundancy in the network when used with Flex Links. If the link is lost on the primary interface, connectivity is transparently switched to the secondary interface.

As shown in Figure 15-4, switches that could be Cisco ME 3400CGS 2520 switches are used as user-facing provider edge (UPE) switches in a customer site at the edge of the provider network connected to a Customer Premises Equipment (CPE) switch. The UPE switches are connected to the provider edge (PE) switches in the service provider (SP) network. Customer devices, such as clients, connected to the CPE switch have multiple connections to the SP network. This configuration ensures

that the traffic flow is balanced from the customer site to the SP and the reverse. Ports connected to the CPE are referred to as downstream ports, and ports connected to PE switches are referred to as upstream ports.

- UPE switch A provides links to the CPE through link-state group 1. Port 1 and port 2 are connected to the CPE. Port 3 and port 4 are connected to PE switch A through link-state group 1.
- UPE switch B provides links to the CPE through link-state group 2. Port 1 and port 2 are connected to CPE. Port 3 and 4 are connected to PE switch A through link-state group 2.

Figure 15-4 Typical Link-State Tracking Configuration



When you enable link-state tracking on the switch, the link state of the downstream ports is bound to the link state of one or more of the upstream ports. After you associate a set of downstream ports to a set of upstream ports, if all of the upstream ports become unavailable, link-state tracking automatically puts the associated downstream ports in an error-disabled state. This causes the CPE primary interface to failover to the secondary interface.

If the PE switch fails, the cables are disconnected, or the link is lost, the upstream interfaces can lose connectivity. When link-state tracking is not enabled and the upstream interfaces lose connectivity, the link states of the downstream interfaces remain unchanged. The CPE is not aware that upstream connectivity has been lost and does not failover to the secondary interface.

An interface can be an aggregation of ports (an EtherChannel), a single physical port in access or trunk mode, or routed ports. These interfaces can be bundled together, and each downstream interface can be associated with a single group consisting of multiple upstream interfaces, referred to as a link-state group.

In a link-state group, the link state of the downstream interfaces is dependent on the link state of the upstream interfaces. If all of the upstream interfaces in a link-state group are in the link-down state, the associated downstream interfaces are forced into the link-down state. If any one of the upstream interfaces in the link-state group in the link-up state, the associated downstream interfaces can change to or remain in a link-up state.

For example, in Figure 14-4, downstream interfaces 1 and 2 on UPE switch A are defined in link-state group 1 with upstream interfaces 3 and 4. Similarly, downstream interfaces 1 and 2 on UPE switch B are defined in link-state group 2 with upstream interfaces 3 and 4.

If the link is lost on upstream interface 3, the link states of downstream interfaces 1 and 2 do not change. If upstream interface 4 also loses link, downstream interfaces 1 and 2 change to the link-down state. The CPE switch stops forwarding traffic to PE switch A and starts to forward traffic to PE switch B.

You can recover a downstream interface link-down condition by removing the failed downstream port from the link-state group. To recover multiple downstream interfaces, disable the link-state group.

Configuring Link-State Tracking

Default Link-State Tracking Configuration

There are no link-state groups defined, and link-state tracking is not enabled for any group.

Link-State Tracking Configuration Guidelines

- An interface that is defined as an upstream interface cannot also be defined as a downstream interface in the same or a different link-state group. The reverse is also true.
- An interface cannot be a member of more than one link-state group.
- You can configure only two link-state groups per switch module.

Configuring Link-State Tracking

Beginning in privileged EXEC mode, follow these steps to configure a link-state group and to assign an interface to a group:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Create a link-state group, and enable link-state tracking. The group number can be 1 to 2; the default is 1.	**link state track** *number*
Step 3	Specify a physical interface or range of interfaces to configure, and enter interface configuration mode.	**interface** *interface-id*

	Step	Command
	Valid interfaces include switch ports in access or trunk mode (IEEE 802.1q), routed ports, or multiple ports bundled into an upstream EtherChannel interface (static or LACP), also in trunk mode. Do not enable link-state tracking on individual interfaces that will be part of a downstream Etherchannel interface.	
Step 4	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.	**no shutdown**
Step 5	Specify a link-state group, and configure the interface as either an **upstream** or **downstream** interface in the group.The group number can be 1 to 2; the default is 1.	**link state group** [*number*] {**upstream** | **downstream**}
Step 6	Return to privileged EXEC mode.	**end**
Step 7	Verify your entries.	**show running-config**
Step 8	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

This example shows how to create a link-state group and configure the interfaces:

```
Switch# configure terminal
Switch(config)# link state track 1
Switch(config)# interface range fastethernet/0/9 -10
Switch(config-if)# link state group 1 upstream
Switch(config-if)# interface fastethernet0/1
Switch(config-if)# link state group 1 downstream
Switch(config-if)# interface fastethernet0/3
Switch(config-if)# link state group 1 downstream
Switch(config-if)# interface fastethernet0/5
Switch(config-if)# link state group 1 downstream
Switch(config-if)# end
```

To disable a link-state group, use the **no link state track** *number* global configuration command.

Displaying Link-State Tracking Status

Use the **show link state group** command to display the link-state group information. Enter this command without keywords to display information about all link-state groups. Enter the group number to display information specific to the group. Enter the detail keyword to display detailed information about the group.

This is an example of output from the **show link state group 1** command:

```
Switch> show link state group 1

Link State Group: 1      Status: Enabled, Down
```

This is an example of output from the **show link state group detail** command:

```
Switch> show link state group detail

(Up):Interface up   (Dwn):Interface Down   (Dis):Interface disabled

Link State Group: 1 Status: Enabled, Down
Upstream Interfaces : Fa0/15(Dwn) Fa0/16(Dwn)
Downstream Interfaces : Fa0/11(Dis) Fa0/12(Dis) Fa0/13(Dis) Fa0/14(Dis)

Link State Group: 2 Status: Enabled, Down
Upstream Interfaces : Fa0/15(Dwn) Fa0/16(Dwn) Fa0/17(Dwn)
Downstream Interfaces : Fa0/11(Dis) Fa0/12(Dis) Fa0/13(Dis) Fa0/14(Dis)
(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
```

For detailed information about the fields in the display, see the command reference for this release.

MODBUS TCP Configuration

This chapter provides the following sections:

Understanding MODBUS TCP

Use Modicon Communication Bus (MODBUS) TCP over an Ethernet network when connecting the switch module to devices such as intelligent electronic devices (IEDs), distributed controllers, substation routers, Cisco IP Phones, Cisco Wireless Access Points, and other network devices such as redundant substation switches.

MODBUS is a serial communications protocol for client-server communication between a switch module (server) and a device in the network running MODBUS client software (client). You can use MODBUS to connect a computer to a remote terminal unit (RTU) in supervisory control and data acquisition (SCADA) systems.

The client can be an IED or a human machine interface (HMI) application that remotely configure and manage devices running MODBUS TCP. The switch module functions as the server.

The CGR 2010 ESM encapsulates a request or response message in a MODBUS TCP application data unit (ADU). A client sends a message to a TCP port on the switch module. The default port number is **502**.

Note For information about the registers that a client can query on a switch module that functions as a MODBUS TCP server, see Appendix C, "MODBUS TCP Registers."

MODBUS and Security

If a firewall or other security services are enabled, the switch module TCP port might be blocked, and the switch module and the client cannot communicate.

If a firewall and other security services are disabled, a denial-of-service attack might occur on the switch module.

- To prevent a denial-of-service attack and to allow a specific client to send messages to the switch module (server), you can use this standard access control list (ACL) that permits traffic only from the assigned source IP address *10.1.1.n*:

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 1 in
!
access-list 1 permit 10.1.1.0 0.0.0.255
```

- To configure quality of service (QoS) to set the rate-limit for MODBUS TCP traffic:

```
interface FastEthernet0/1
ip address 10.1.1.1 255.255.255.0
ip access-group 1 in
 rate-limit input access-group 101 8000 8000 8000 conform-action transmit
exceed-action drop
!
access-list 101 permit tcp 10.1.1.0 0.0.0.255 any eq 502
```

Multiple Request Messages

The switch module can receive multiple request messages from clients and respond to them simultaneously.

You can set the number of client connections from 1 to 5. The default is 1.

Configuring the Switch Module as the MODBUS TCP Server

Defaults

- Switch module is not configured as a MODBUS TCP server
- TCP switch module port number is 502
- Number of simultaneous connection requests is 1

Enabling MODBUS TCP on the Switch Module

Beginning in privileged EXEC mode:

	Step	Command
Step 1	Enters global configuration mode.	`configure terminal`
Step 2	Enables MODBUS TCP on the switch module	`scada modbus tcp server`

	Step	Command
Step 3	(Optional) Sets the TCP port to which clients send messages. The range for *tcp-port-number* is 1 to 65535. The default is 502.	**scada modbus tcp server port** *tcp-port-number*
Step 4	(Optional) Sets the number of simultaneous connection requests sent to the switch module. The range for *connection-requests* is 1 to 5. The default is 1.	**scada modbus tcp server connection** *connection-requests*
Step 5	Returns to privileged EXEC mode.	**end**
Step 6	Displays the server information and statistics.	**show scada modbus tcp server**
Step 7	(Optional) Saves your entries in the configuration file.	**copy running-config startup config**

To disable MODBUS on the switch module and return to the default settings, enter the **no scada modbus tcp server** global configuration command.

To clear the server and client statistics, enter the **clear scada modbus tcp server statistics** privileged EXEC command.

After you enable MODBUS TCP on the switch module, this warning appears:

```
WARNING: Starting Modbus TCP server is a security risk.
Please understand the security issues involved before
proceeding further. Do you still want to start the
server? [yes/no]:
```

To add security when using MODBUS TCP, configure an ACL to permit traffic from specific clients or configure QoS to rate-limit traffic.

Displaying MODBUS TCP Information

Table 16-1 show scada modbus Command

Command	Description
show scada modbus tcp server	Displays the server information and statistics
show scada modbus tcp server connections	Displays the client information and statistics

SDM Template Configuration

This chapter describes how to configure the Switch Database Management (SDM) templates on the CGR 2010 ESM. SDM template configuration is supported only when the switch module is running the IP services image.

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

Understanding the SDM Templates

If the switch module is running the IP services image, you can use SDM templates to optimize system resources in the switch module to support specific features, depending on how the switch module is used in the network. The SDM templates allocate TCAM (Ternary Content Addressable Memory) 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 Switch modules running the LAN base image support only the Layer-2 template

- 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 module is being used for Layer-2 forwarding. When you select the layer-2 template on a switch module 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 only on switch modules running the IP services image. If you do not use the default template when routing is enabled on the switch module, 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 17-2.

Table 17-1 shows the approximate number of each resource supported in each of the two IPv4 templates for a switch module running the IP services image. 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 module performance.

Table 17-1 Approximate Number of Feature Resources Allowed by Each Template

Resource	Layer-2 Template	Default Template
Unicast MAC addresses	2 K	8 K
IPv4 IGMP groups + multicast routes (default only)	1 K	0.25 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	0.375 K
IPv4 or MAC security ACEs	1 K	0.375 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 Chapter 39, “Configuring IPv6 Unicast Routing” in the *Cisco CGS 2520 Software Configuration Guide*. For information about configuring IPv6 ACLs, see Chapter 41, “Configuring IPv6 ACLs” in the *Cisco CGS 2520 Software Configuration Guide.*

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 module 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 module.
- 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 module.
- 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 module.

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 17-2 defines the approximate feature resources allocated by each dual template. Template estimations are based on a switch module with 8 routed interfaces and approximately 1000 VLANs.

Table 17-2 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	8 K	1 K	4 K
IPv4 IGMP groups and multicast routes	0.25 K	0.5 K	1 K
Total IPv4 unicast routes:	0	2 K	0
• Directly connected IPv4 hosts	-	1 K	-
• Indirect IPv4 routes	- K	1 K	-
IPv6 multicast groups	0.375 K	0.625 K	1.125 K
Total IPv6 unicast routes:	0	2.75 K	0
• Directly connected IPv6 addresses	0	1 K	0
• Indirect IPv6 unicast routes	0	0.625 K	0
IPv4 policy-based routing ACEs	0	0.125 K	0
IPv4 or MAC QoS ACEs (total)	0.375 K	0.375 K	0.5 K
IPv4 or MAC security ACEs (total)	0.375 K	0.125 K	0.5 K
IPv6 policy-based routing ACEs[1]	0	0.25 K	0
IPv6 QoS ACEs	0	0	0.5 K
IPv6 security ACEs	0.125 K	0.25 K	0.5 K

1. IPv6 policy-based routing is not supported.

Configuring the Switch Module SDM Template

Default SDM Template

The default template for a switch module running the IP services image is the default template.

The default (and only) template supported on switch modules running the LAN base image is the Layer-2 template.

SDM Template Configuration Guidelines

Follow these guidelines when selecting and configuring SDM templates:

- You must reload the switch module for the configuration to take effect.
- If you are using the switch module 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 module. 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 module. 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 the dual-stack templates if you plan to forward only IPv4 traffic.

Setting the SDM Template

Beginning in privileged EXEC mode, follow these steps to use the SDM template to select a template on a switch module running the IP services image:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Specify the SDM template to be used on the switch module: 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 module.	**sdm prefer** {**default** | **dual-ipv4-and-ipv6** {**default** | **routing** | **vlan**} | **layer-2**}
Step 3	Return to privileged EXEC mode.	**end**
Step 4	Reload the operating system.	**reload**

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

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

```
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 0 routed interfaces and 1024 VLANs.

number of unicast mac addresses:8K
number of IPv4 IGMP groups + multicast routes:0.25K
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:                      0.375K
number of IPv4/MAC security aces:0.375K
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 module with the Layer-2 template:

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

Displaying the SDM Templates

Use the **show sdm prefer** privileged EXEC command with no parameters to display the active template. Use the **show sdm prefer** [**default** | **dual-ipv4-and-ipv6** {**default** | **routing** | **vlan**} | **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:8K
number of IPv4 IGMP groups + multicast routes:0.25K
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:                      0.375K
number of IPv4/MAC security aces:0.375K.
```

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:2K
number of IPv4 IGMP groups:1K
number of IPv4 multicast routes:1K
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:1K
number of IPv4 IGMP groups + multicast routes:0.5K
number of IPv4 unicast routes: 2K
number of directly-connected IPv4 hosts:1K
number of indirect IPv4 routes:1K
number of IPv6 multicast groups:0.625K
number of directly-connected IPv6 addresses:1K
number of indirect IPv6 unicast routes:0.625K
number of IPv4 policy based routing aces:0.125K
number of IPv4/MAC qos aces:0.375K
number of IPv4/MAC security aces:0.125K
number of IPv6 policy based routing aces:0
number of IPv6 qos aces:0.25K
number of IPv6 security aces:0.25K
```

Troubleshooting

This chapter describes how to identify and resolve software problems related to the Cisco IOS software on the CGR 2010 ESM.

You can use the command-line interface (CLI) to identify and solve problems.

Note For complete syntax and usage information for the commands used in this chapter, see the command reference for this release and the *Cisco IOS Command Summary, Release 12.2*.

Recovering from a Software Failure

The switch module software can be corrupted during an upgrade by downloading the wrong file to the switch module, and by deleting the image file. In all of these cases, the switch module does not pass the power-on self-test (POST), and there is no connectivity.

Recovery Procedure at 115200 Baud Line Speed

This procedure uses the Xmodem Protocol at 115200 baud line speed to recover from a corrupt or wrong image file. There are many software packages that support the Xmodem Protocol, and this procedure is largely dependent on the emulation software that you are using.

Because there is no console port on the switch module, recovery must be done from the CGR 2010 router.

For more information, see "*Recovering from a Corrupted Software Image Using Xmodem*" in the *Cisco Enhanced EtherSwitch Services Modules Configuration Guide*.

Recovering from a Lost or Forgotten Password

If you lose or forget your password, you can delete the switch module password and set a new one.

Before you begin, make sure that:

- You have physical access to the switch module.
- At least one switch module port is enabled and it is not connected to a device.

To delete the switch module password and set a new one, follow these steps:

Step 1 Press the **Express Setup** button until the SETUP LED blinks green and the LED of an available downlink port blinks green.

a. If no switch module downlink port is available for your PC or laptop connection, disconnect a device from one of the other downlink ports.

b. Press the **Express Setup** button again until the SETUP LED and the port LED blink green.

Step 2 Connect your PC or laptop to the port with the blinking green LED.

The SETUP LED and the switch module downlink port LED stop blinking and stay solid green.

Step 3 Press and hold the **Express Setup** button.

Notice that the SETUP LED starts blinking green again.

a. Continue holding the button until the SETUP LED turns solid green (approximately 5 seconds). Release the Express Setup button immediately.

This procedure deletes the password without affecting any other configuration settings. You can now access the switch module without a password through the console port or by using the device manager.

Step 4 Enter a new password through the device manager by using the Express Setup window or through the command line interface by using the **enable secret** global configuration command.

Preventing Autonegotiation Mismatches

The IEEE 802.3ab autonegotiation protocol manages the switch module settings for speed (10, 100, and 1000 Mbps, excluding SFP module ports) and duplex (half or full). There are situations when this protocol can incorrectly align these settings, reducing performance. A mismatch occurs under these circumstances:

- A manually set speed or duplex parameter is different from the manually set speed or duplex parameter on the connected port.
- A port is set to autonegotiate, and the connected port is set to full duplex with no autonegotiation.

To maximize switch module performance and ensure a link, follow one of these guidelines when changing the settings for duplex and speed:

- Let both ports autonegotiate both speed and duplex.
- Manually set the speed and duplex parameters for the ports on both ends of the connection.

Note If a remote device does not autonegotiate, configure the duplex settings on the two ports to match. The speed parameter can adjust itself even if the connected port does not autonegotiate.

Troubleshooting Power over Ethernet Switch Module Ports

These sections describe how to troubleshoot Power over Ethernet (PoE) ports.

Disabled Port Caused by Power Loss

If a powered device (such as a Cisco IP Phone 7910) that is connected to a PoE switch module port and is powered by an AC power source loses power from the AC power source, the device might enter an error-disabled state.

Recovering from an Error-Disabled State

1. Enter the **shutdown** interface configuration command.
2. Then enter the **no shutdown** interface command.

You can also configure automatic recovery on the switch module to recover from the error-disabled state. The **errdisable recovery cause loopback** and the **errdisable recovery interval** *seconds* global configuration commands automatically take the interface out of the error-disabled state after the specified period of time.

Use these commands, described in the command reference for this release, to monitor the PoE port status:

- **show controllers power inline** privileged EXEC command
- **show power inline** privileged EXEC command
- **debug ilpower** privileged EXEC command

Disabled Port Caused by False Link-Up

If a Cisco powered device is connected to a port and you configure the port by using the **power inline never interface** configuration command, a false link-up can occur, placing the port into an error-disabled state.

To take the port out of the error-disabled state, enter the **shutdown interface** and the **no shutdown interface** configuration commands.

Do not connect a Cisco powered device to a port that has been configured with the **power inline never** command.

SFP Module Security and Identification

Cisco small form-factor pluggable (SFP) modules have a serial EEPROM that contains the module serial number, the vendor name and ID, a unique security code, and cyclic redundancy check (CRC). When an SFP module is inserted in the switch module, the switch module software reads the EEPROM to verify the serial number, vendor name and vendor ID, and recompute the security code and CRC. If the serial number, the vendor name or vendor ID, the security code, or CRC is invalid, the software generates a security error message and places the interface in an error-disabled state.

Note The security error message references the GBIC_SECURITY facility. The switch module supports SFP modules and does not support GBIC modules. Although the error message text refers to GBIC interfaces and modules, the security messages actually refer to the SFP modules and module interfaces. For more information about error messages, see the system message guide *f*or this release.

Non-Cisco SFP Module

1. Remove the SFP module from the switch module, and replace it with a Cisco module.
2. After inserting a Cisco SFP module, use the **errdisable recovery cause gbic-invalid** global configuration command to verify the port status, and enter a time interval for recovering from the error-disabled state.

   After the elapsed interval, the switch module brings the interface out of the error-disabled state and retries the operation.

   For more information about the **errdisable recovery** command, see the command reference for this release.

Cisco SFP Module

If the module is identified as a Cisco SFP module, but the system is unable to read vendor-data information to verify its accuracy, an SFP module error message is generated.

In this case, you should remove and re-insert the SFP module. If it continues to fail, the SFP module might be defective.

Monitoring SFP Module Status

You can check the physical or operational status of an SFP module by using the **show interfaces transceiver** privileged EXEC command. This command shows the operational status, such as the temperature and the current for an SFP module on a specific interface and the alarm status.

Note The **show interfaces transceiver** command only works if the SFP supports DOM.

You can also use the command to check the speed and the duplex settings on an SFP module. For more information, see the **show interfaces transceiver** command in the command reference for this release.

Monitoring Temperature and Configuring the Yellow Threshold

The CGR 2010 ESM includes sensors that measure and monitor the status and internal temperature of critical components. Internal component temperatures are measured for the central processor, internal components, and interface cards.

The measured temperature is compared to predetermined threshold limits and, if the temperature does not fall within the limits, the information is recorded and a warning sent to the system administrator by means of Simple Network Management Protocol (SNMP) traps until the temperature falls back to its normal range.

- Use the **show env temperature status** privileged EXEC command to display the current temperature value, state, and thresholds of the switch's CPU and Ethernet board (see Table 18-1 below). The temperature value is the temperature in the switch module (not the external temperature). If the temperature exceeds the threshold, a warning message is sent.
- You can configure the yellow threshold level (in Celsius) by using the **system env temperature threshold yellow** *value* global configuration command to set the difference between the yellow and red thresholds. You cannot configure the green or red thresholds (see "Configuring the Yellow Threshold" below for details).

Temperature Show Commands

The switch module monitors the temperature conditions to determine the health of the power supplies. The temperature value is the temperature in the switch module (not the external temperature).

Table 18-1 describes the **Show** commands that monitor the switch's temperature:

Table 18-1 Temperature Show Commands

Command	Function
`Switch# show env all | temperature status`	• *all*: Displays all environmental monitor parameters • *temperature status*: Shows temperature status and threshold levels of the switch's CPU and Ethernet board.

Configuring the Yellow Threshold

You cannot configure the green and red thresholds but you can configure the yellow threshold.

Note The yellow thresold is independent for the CPU sensor and Ethernet board sensor. At this time, only the CPU yellow threshold can be changed.

Use the **system env temperature threshold yellow** *value* global configuration command to specify the difference between the yellow and red threshold values and to configure the yellow threshold (in Celsius). The range is 20 to 25. The default value is 20.

For example, if the red threshold is 60 degrees C and you want to configure the yellow threshold as 51 degrees C, set the difference between the thresholds as 15 by using the **system env temperature threshold yellow 9** command.

Use the no form of this command to return to the default value.

Note The default red threshold is 100 degrees C; the default yellow threshold is 94 degrees C for the CPU board; and 95 degrees C for the Ethernet board.

Using Ping

Understanding Ping

The switch module supports IP ping, which you can use to test connectivity to remote hosts. Ping sends an echo request packet to an address and waits for a reply.

The switch module also provides the Control Plane Security feature, which by default drops ping response packets received on user network interfaces (UNIs) or enhanced network interfaces (ENIs). However, methods are available to ping successfully from the switch module to a host connected to a UNI or ENI.

Control Plane Security does not drop ping response packets to or from network node interfaces (NNIs), and no special configuration is required to enable pings to or from hosts connected to NNIs.

Using Ping

Beginning in privileged EXEC mode, use the **ping** command to ping another device on the network from the switch module:

Command	Description
ping [*host* | *address]*	Ping a remote host by supplying the hostname or IP network address. **Note** Though other protocol keywords are available with the **ping** command, they are not supported in this release.

Note Ping is not supported on a UNI or ENI configured as an IEEE 802.1Q tunnel port. Ping is supported on NNIs on all software images.

It is important to note that the software images available for the switch module provide different options for pinging a host connected to a UNI or ENI.

The next sections apply to both access ports and trunk ports.

All Software Versions

For all software images for the switch module, you can use a Layer 3 service policy to enable pings from the switch module to a host connected to a UNI or ENI.

Note For a switch module running the IP services image, IP routing is not enabled by default and does not have to be enabled to use a Layer 3 service policy.

This example is one possible configuration:

```
switch# configure terminal
switch(config)# access list 101 permit ip any any
switch(config)# class-map match-any ping-class
switch(config-cmap)# match access-group 101
switch(config-cmap)# exit
switch(config)# policy-map ping-policy
switch(config-pmap)# class ping-class
switch(config-pmap-c)# police 1000000
switch(config-pmap-c)# exit
switch(config-pmap)# exit
switch(config)# int fa0/1
switch(config-if)# service-policy input ping-policy
switch(config-if)# switchport access vlan 2
switch(config-if)# no shut
switch(config-if)# exit
switch(config)# int vlan 2
switch(config-if)# ip address 192.168.1.1 255.255.255.0
switch(config-if)# end
switch# ping 192.168.1.2
```

IP Services Image

When your switch module is running the IP services image, you can use any of these methods:

- Apply a Layer 3 service policy to a UNI or ENI.
- Enable IP routing globally and ping from a Switch Virtual Interface (SVI).
- Enable IP routing and ping from a routed port.

For a sample configuration of how to add a Layer 3 service policy to a UNI or ENI, see the "All Software Versions" section on page 18-7.

For examples using IP routing and pinging from an SVI or a routed port, see the next sections.

IP Routing and SVI

IP routing is only supported when the switch module is running the IP services image.

You can use this configuration to enable IP routing and enable pings from an SVI to a host connected to a UNI or ENI.

```
Switch# configure terminal
Switch(config)# ip routing
Switch(config)# int fa0/1
Switch(config-if)# switchport access vlan 2
Switch(config-if)# no shutdown
Switch(config-if)# int vlan 2
Switch(config-if)# ip address 192.168.1.1 255.255.255.0
Switch(config-if)# end
Switch# ping 192.168.1.2
```

With this configuration, a host with an IP address of 192.168.1.2 can be pinged from the switch module.

IP Routing and Routed Port

You can use this configuration to enable IP routing, change a switchport to a routed port, and permit pings from the switch module to a connected host:

```
switch# configure terminal
switch(config)# int fa0/1
switch(config-if)# no switchport
switch(config-if)# ip address 192.168.1.1 255.255.255.0
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# ip routing
switch(config)# end
switch# ping 192.168.1.2
```

Ping Responses

This response is typical of a successful ping to a host:

```
Switch# ping 72.20.52.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.20.52.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Switch#
```

An unsuccessful ping results in this message:

```
Switch# ping 72.20.52.3
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.20.52.3, timeout is 2 seconds:
. . . . .
Success rate is 0 percent (0/5)
```

Summary

Keep these guidelines in mind while pinging:

- IP routing is available only with the IP services image and is disabled by default.
- To ping a host in a different IP subnetwork from the switch module, you must have IP routing configured to route between the subnets, and a static route to the destination might also be appropriate.
- All software versions can use a Layer 3 service policy to permit pings to and from a host connected to a UNI or ENI. For more information about policy maps, see the "Input and Output Policies" section on page 14-4.

If your switch module is running the IP services image, use one of these methods to ping a host connected to a UNI or ENI:

- Use a Layer 3 service policy to permit pings to and from a host connected to a UNI or ENI.
- Enable global IP routing and configure a port as a routed port by using the **no switchport** interface configuration command.
- Enable global IP routing, create an SVI, and assign an IP address to it

Using Layer 2 Traceroute

Understanding Layer 2 Traceroute

The Layer 2 traceroute feature allows the switch module to identify the physical path that a packet takes from a source device to a destination device. Layer 2 traceroute supports only unicast source and destination MAC addresses. It finds the path by using the MAC address tables of the switches in the path. When the switch module detects a device in the path that does not support Layer 2 traceroute, the switch module continues to send Layer 2 trace queries and lets them time out.

Note Layer 2 traceroute is available only on NNIs.

The switch module can only identify the path from the source device to the destination device. It cannot identify the path that a packet takes from source host to the source device or from the destination device to the destination host.

Layer 2 Traceroute Usage Guidelines

- Cisco Discovery Protocol (CDP) must be enabled on all the devices in the network. For Layer 2 traceroute to function properly, do not disable CDP.

Note CDP is enabled by default on NNIs. You can enable CDP on ENIs, but UNIs do not support CDP.

  If any devices in the physical path are transparent to CDP, the switch module cannot identify the path through these devices.

- A switch module is reachable from another switch module when you can test connectivity by using the **ping** privileged EXEC command. All switches in the physical path must be reachable from each other.
- The maximum number of hops identified in the path is ten.
- You can enter the **traceroute mac** or the **traceroute mac ip** privileged EXEC command on a switch module that is not in the physical path from the source device to the destination device. All switches in the path must be reachable from this switch module.
- The **traceroute mac** command output shows the Layer 2 path only when the specified source and destination MAC addresses belong to the same VLAN. If you specify source and destination MAC addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.
- If you specify a multicast source or destination MAC address, the path is not identified, and an error message appears.
- If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong. If the VLAN is not specified, the path is not identified, and an error message appears.
- The **traceroute mac ip** command output shows the Layer 2 path when the specified source and destination IP addresses belong to the same subnet. When you specify the IP addresses, the switch module uses the Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.
  - If an ARP entry exists for the specified IP address, the switch module uses the associated MAC address and identifies the physical path.
  - If an ARP entry does not exist, the switch module sends an ARP query and tries to resolve the IP address. If the IP address is not resolved, the path is not identified, and an error message appears.
- When multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port), the Layer 2 traceroute feature is not supported. When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.
- This feature is not supported in Token Ring VLANs.

Displaying the Physical Path

You can display the physical path that a packet takes from a source device to a destination device by using one of these privileged EXEC commands:

- **tracetroute mac** [**interface** *interface-id*] {*source-mac-address*} [**interface** *interface-id*] {*destination-mac-address*} [**vlan** *vlan-id*] [**detail**]

- **tracetroute mac ip** {*source-ip-address* | *source-hostname*}{*destination-ip-address* | *destination-hostname*} [**detail**]

Note Layer 2 traceroute is available only on NNIs.

For more information, see the command reference for this release.

Using IP Traceroute

Understanding IP Traceroute

You can use IP traceroute to identify the path that packets take through the network on a hop-by-hop basis. The command output displays all network layer (Layer 3) devices, such as routers, that the traffic passes through on the way to the destination.

Your switches can participate as the source or destination of the **traceroute** privileged EXEC command and might or might not appear as a hop in the **traceroute** command output. If the switch module is the destination of the traceroute, it is displayed as the final destination in the output. Intermediate switches do not show up in the output if they are only bridging the packet from one port to another within the same VLAN. However, if the intermediate switch module is a multilayer switch module that is routing a particular packet, this switch module shows up as a hop in the output.

The **traceroute** privileged EXEC command uses the Time To Live (TTL) field in the IP header to cause routers and servers to generate specific return messages. Traceroute starts by sending a User Datagram Protocol (UDP) datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it drops the datagram and sends an Internet Control Message Protocol (ICMP) time-to-live-exceeded message to the sender. Traceroute finds the address of the first hop by examining the source address field of this message.

To identify the next hop, traceroute sends a UDP packet with a TTL value of 2. The first router decrements the TTL field by 1 and sends the datagram to the next router. The second router sees a TTL value of 1, discards the datagram, and returns the time-to-live-exceeded message to the source. This process continues until the TTL is incremented to a value large enough for the datagram to reach the destination host (or until the maximum TTL is reached).

To learn when a datagram reaches its destination, traceroute sets the UDP destination port number in the datagram to a very large value that the destination host is unlikely to be using. When a host receives a datagram destined to itself containing a destination port number that is unused locally, it sends an ICMP *port-unreachable* error to the source. Because all errors except port-unreachable errors come from intermediate hops, the receipt of a port-unreachable error means that this message was sent by the destination port.

Executing IP Traceroute

Beginning in privileged EXEC mode, follow this step to trace that the path packets take through the network:

Command	Description
traceroute ip *host*	Trace the path that packets take through the network.

Note Though other protocol keywords are available with the **traceroute** privileged EXEC command, they are not supported in this release.

This example shows how to perform a **traceroute** to an IP host:

```
Switch# traceroute ip 171.9.15.10

Type escape sequence to abort.
Tracing the route to 171.69.115.10
  1 172.2.52.1 0 msec 0 msec 4 msec
  2 172.2.1.203 12 msec 8 msec 0 msec
  3 171.9.16.6 4 msec 0 msec 0 msec
  4 171.9.4.5 0 msec 4 msec 0 msec
  5 171.9.121.34 0 msec 4 msec 4 msec
  6 171.9.15.9 120 msec 132 msec 128 msec
  7 171.9.15.10 132 msec 128 msec 128 msec
Switch
```

The display shows the hop count, IP address of the router, and the round-trip time in milliseconds for each of the three probes that are sent.

Table 18-2 Traceroute Output Display Characters

Character	Description
*	Probe timed out
?	Unknown packet type
A	Administratively unreachable—usually this output means that an access list is blocking traffic
H	Host unreachable
N	Network unreachable
P	Protocol unreachable
Q	Source quench
U	Port unreachable

Using TDR

Understanding TDR

You can use the Time Domain Reflector (TDR) feature to diagnose and resolve cabling problems. When running TDR, a local device sends a signal through a cable and compares the reflected signal to the initial signal.

On the CGR 2010 ESM, TDR is supported only on the copper Ethernet 10/100 ports or on dual-purpose ports configured to either 10 Mbps or 100 Mbps ports and media-type RJ-45.

TDR can detect these cabling problems:

- Open, broken, or cut twisted-pair wires—The wires are not connected to the wires from the remote device.
- Shorted twisted-pair wires—The wires are touching each other or the wires from the remote device. For example, a shorted twisted pair can occur if one wire of the twisted pair is soldered to the other wire.

If one of the twisted-pair wires is open, TDR can find the length at which the wire is open.

Use TDR to diagnose and resolve cabling problems in these situations:

- Replacing a switch module
- Setting up a wiring closet
- Troubleshooting a connection between two devices when a link cannot be established or when it is not operating properly

Running TDR and Displaying the Results

To run TDR, enter the **test cable-diagnostics tdr interface** *interface-id* privileged EXEC command:

To display the results, enter the **show cable-diagnostics tdr interface** *interface-id* privileged EXEC command. For a description of the fields in the display, see the command reference for this release.

Note TDR is supported only on the copper Ethernet 10/100 ports or on dual-purpose ports configured as 10/100/100 ports by using the RJ-45 connector.

Using Debug Commands

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. It is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Note For complete syntax and usage information for specific **debug** commands, see the command reference for this release.

Enabling Debugging on a Specific Feature

All **debug** commands are entered in privileged EXEC mode, and most **debug** commands take no arguments. For example, beginning in privileged EXEC mode, enter this command to enable the debugging for Switched Port Analyzer (SPAN):

```
Switch# debug span-session
```

The switch module continues to generate output until you enter the **no** form of the command.

If you enable a **debug** command and no output appears, consider these possibilities:

- The switch module might not be properly configured to generate the type of traffic that you want to monitor. Use the **show running-config** command to check its configuration.
- Even if the switch module is properly configured, it might not generate the type of traffic that you want to monitor during the particular period that debugging is enabled. Depending on the feature you are debugging, you can use commands such as the TCP/IP **ping** command to generate network traffic.

To disable debugging of SPAN, enter this command in privileged EXEC mode:

```
Switch# no debug span-session
```

Alternately, in privileged EXEC mode, you can enter the **undebug** form of the command:

```
Switch# undebug span-session
```

To display the state of each debugging option, enter this command in privileged EXEC mode:

```
Switch# show debugging
```

Enabling All-System Diagnostics

Beginning in privileged EXEC mode, enter this command to enable all-system diagnostics:

```
Switch# debug all
```

Caution Because debugging output takes priority over other network traffic, and because the **debug all** privileged EXEC command generates more output than any other **debug** command, it can severely diminish switch module performance or even render it unusable. In virtually all cases, it is best to use more specific **debug** commands.

The **no debug all** privileged EXEC command disables all diagnostic output. Using the **no debug all** command is a convenient way to ensure that you have not accidentally left any **debug** commands enabled.

Redirecting Debug and Error Message Output

By default, the network server sends the output from **debug** commands and system error messages to the console. If you use this default, you can use a virtual terminal connection to monitor debug output instead of connecting to the console port.

Possible destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. The syslog format is compatible with 4.3 Berkeley Standard Distribution (BSD) UNIX and its derivatives.

Note Be aware that the debugging destination you use affects system overhead. Logging messages to the console produces very high overhead, whereas logging messages to a virtual terminal produces less overhead. Logging messages to a syslog server produces even less, and logging to an internal buffer produces the least overhead of any method.

Using the *show platform forward* Command

The output from the **show platform forward** privileged EXEC command provides some useful information about the forwarding results if a packet entering an interface is sent through the system. Depending upon the parameters entered about the packet, the output provides lookup table results and port maps used to calculate forwarding destinations, bitmaps, and egress information.

Note For more syntax and usage information for the **show platform forward** command, see the switch module command reference for this release.

Most of the information in the output from the command is useful mainly for technical support personnel, who have access to detailed information about the switch module ASICs. However, packet forwarding information can also be helpful in troubleshooting.

This is an example of the output from the **show platform forward** command on Gigabit Ethernet port 1 in VLAN 5 when the packet entering that port is addressed to unknown MAC addresses. The packet should be flooded to all other ports in VLAN 5.

```
Switch# show platform forward gigabitethernet0/1 vlan 5 1.1.1 2.2.2 ip 13.1.1.1 13.2.2.2
udp 10 20
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
 Lookup                    Key-Used                    Index-Hit  A-Data
InptACL  40_0D020202_0D010101-00_40000014_000A0000     01FFA   03000000
L2Local  80_00050002_00020002-00_00000000_00000000     00C71   0000002B
Station Descriptor:02340000, DestIndex:0239, RewriteIndex:F005

========================================
Egress:Asic 2, switch 1
Output Packets:

----------------------------------------
Packet 1
 Lookup                    Key-Used                    Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000     01FFE   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Gi0/1    0005 0001.0001.0001  0002.0002.0002

----------------------------------------
Packet 2
 Lookup                    Key-Used                    Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000     01FFE   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Gi0/2    0005 0001.0001.0001  0002.0002.0002

----------------------------------------
<output truncated>
----------------------------------------
Packet 10
 Lookup                    Key-Used                    Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000     01FFE   03000000
Packet dropped due to failed DEJA_VU Check on Gi0/2
```

This is an example of the output when the packet coming in on Gigabit Ethernet port 1 in VLAN 5 is sent to an address already learned on the VLAN on another port. It should be forwarded from the port on which the address was learned.

```
Switch# show platform forward gigabitethernet0/1 vlan 5 1.1.1 0009.43a8.0145 ip 13.1.1.1
13.2.2.2 udp 10 20
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
 Lookup                    Key-Used                    Index-Hit  A-Data
InptACL  40_0D020202_0D010101-00_40000014_000A0000     01FFA   03000000
L2Local  80_00050009_43A80145-00_00000000_00000000     00086   02010197
Station Descriptor:F0050003, DestIndex:F005, RewriteIndex:0003

========================================
Egress:Asic 3, switch 1
Output Packets:


----------------------------------------
Packet 1
 Lookup                    Key-Used                    Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000     01FFE   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Gi0/2    0005 0001.0001.0001  0009.43A8.0145
```

This is an example of the output when the packet coming in on Gigabit Ethernet port 1 in VLAN 5 has a destination MAC address set to the router MAC address in VLAN 5 and the destination IP address unknown. Because there is no default route set, the packet should be dropped.

```
Switch# show platform forward gigabitethernet0/1 vlan 5 1.1.1 03.e319.ee44 ip 13.1.1.1
13.2.2.2 udp 10 20
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
 Lookup                    Key-Used                     Index-Hit  A-Data
InptACL  40_0D020202_0D010101-00_41000014_000A0000     01FFA   03000000
L3Local  00_00000000_00000000-90_00001400_0D020202     010F0   01880290
L3Scndr  12_0D020202_0D010101-00_40000014_000A0000     034E0   000C001D_00000000
Lookup Used:Secondary
Station Descriptor:02260000, DestIndex:0226, RewriteIndex:0000
```

This is an example of the output when the packet coming in on Gigabit Ethernet port 1 in VLAN 5 has a destination MAC address set to the router MAC address in VLAN 5 and the destination IP address set to an IP address that is in the IP routing table. It should be forwarded as specified in the routing table.

```
Switch# show platform forward gigabitethernet0/1 vlan 5 1.1.1 03.e319.ee44 ip 110.1.5.5
16.1.10.5
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
 Lookup                    Key-Used                     Index-Hit  A-Data
InptACL  40_10010A05_0A010505-00_41000014_000A0000     01FFA   03000000
L3Local  00_00000000_00000000-90_00001400_10010A05     010F0   01880290
L3Scndr  12_10010A05_0A010505-00_40000014_000A0000     01D28   30090001_00000000
Lookup Used:Secondary
Station Descriptor:F0070007, DestIndex:F007, RewriteIndex:0007

========================================
Egress:Asic 3, switch 1
Output Packets:

----------------------------------------
Packet 1
 Lookup                    Key-Used                     Index-Hit  A-Data
OutptACL 50_10010A05_0A010505-00_40000014_000A0000     01FFE   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Gi0/2    0007 XXXX.XXXX.0246  0009.43A8.0147
```

Using the *crashinfo* File

The crashinfo file saves information that helps Cisco technical support representatives to debug problems that caused the Cisco IOS image to fail (crash). The switch module writes the crash information to the console at the time of the failure, and the file is created the next time you boot the Cisco IOS image after the failure (instead of while the system is failing).

The information in the file includes the Cisco IOS image name and version that failed, a list of the processor registers, and a stack trace. You can provide this information to the Cisco technical support representative by using the **show tech-support** privileged EXEC command.

All crashinfo files are kept in this directory on the flash file system:

flash:/crashinfo/crashinfo_*n* where *n* is a sequence number.

Each new crashinfo file that is created uses a sequence number that is larger than any previously existing sequence number, so the file with the largest sequence number describes the most recent failure. Version numbers are used instead of a timestamp because the switches do not include a real-time clock. You cannot change the name of the file that the system will use when it creates the file. However, after the file is created, you can use the **rename** privileged EXEC command to rename it, but the contents of the renamed file will not be displayed by the **show tech-support** privileged EXEC command. You can delete crashinfo files by using the **delete** privileged EXEC command.

You can display the most recent crashinfo file (that is, the file with the highest sequence number at the end of its filename) by entering the **show tech-support** privileged EXEC command. You also can access the file by using any command that can copy or display files, such as the **more** or the **copy** privileged EXEC command.

Using On-Board Failure Logging

You can use the on-board-failure logging (OBFL) feature to collect information about the switch module. The information includes uptime, temperature, and voltage information and helps Cisco technical support representatives to troubleshoot switch module problems.

This section has this information:

- Understanding OBFL, page 18-18
- Configuring OBFL, page 18-19
- Displaying OBFL Information, page 18-19

Understanding OBFL

By default, OBFL is enabled. It collects information about the switch module and small form-factor pluggable (SFP) modules. The switch module stores this information in the flash memory:

- CLI commands—Record of the OBFL CLI commands that are entered on a switch module
- Environmental data—Unique Device Identifier (UDI) information for a switch module and for all the connected devices: the product identification (PID), the version identification (VID), and the serial number
- Message—Record of the hardware-related system messages generated by a switch module
- Temperature—Temperature of a switch module
- Uptime data—Time when a switch module starts, the reason the switch module restarts, and the length of time the switch module has been running since it last restarted
- Voltage—System voltages of a switch module

You should manually set the system clock or configure it by using Network Time Protocol (NTP).

When the switch module is running, you can retrieve the OBFL data by using the show logging onboard privileged EXEC commands. If the switch module fails, contact your Cisco technical support representative to find out how to retrieve the data.

When an OBFL-enabled switch module is restarted, there is a 10-minute delay before logging of new data begins.

Configuring OBFL

To enable OBFL, use the **hw-module module logging onboard** [**message level** *level*] global configuration command. Use the **message level** *level* parameter to specify the severity of the hardware-related messages that the switch module generates and stores in the flash memory.

To copy the OBFL data to the local network or a specific file system, use the **copy logging onboard module 1** *destination* privileged EXEC command.

Note We recommend that you keep OBFL enabled and that you do not remove the data stored in the flash memory.

Beginning in privileged EXEC mode, follow these steps to enable and configure OBFL. Note that OBLF is enabled by default; you need to enable it only if it has been disabled.

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enable OBFL on the switch module. You can specify these optional parameters: • (Optional) *slot-number*—The slot number is always 1 and is not relevant for the switch module. • (Optional) **message** *level*—Specify the severity level of messages to be generated and stored. The range is from 1 to 7, with 1 being the most severe.	**hw-module module** [*slot-number*] **logging onboard** [**message** *level*]
Step 3	Return to privileged EXEC mode.	**end**
Step 4	(Optional) Copy the OBFL data to the local network or a specific file system. • (Optional) *slot-number*—The slot number is always 1 and is not relevant for the switch module. • *destination*—See the **copy logging onboard module** command for destination options.	**copy logging onboard module** [*slot-number*] *destination*
Step 5	Verify your entries.	**show logging onboard**
Step 6	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

To disable OBFL, use the no **hw-module module 1 logging onboard** [**message** *level*] global configuration command.

To clear all the OBFL data in the flash memory except for the uptime and CLI command information, use the **clear logging onboard** privileged EXEC command.

For more information about the commands in this section, see the command reference for this release.

Displaying OBFL Information

To display the OBFL information, use one or more of the privileged EXEC commands in Table 18-3.

Note When an OBFL-enabled switch module is restarted, there is a 10-minute delay before logging of new data begins.

Table 18-3 Commands for Displaying OBFL Information

Command	Description
show logging onboard clilog	Displays the OBFL CLI commands that were entered on a switch module
show logging onboard environment	Displays the UDI information for a standalone switch module and for all the connected FRU devices: the PID, the VID, and the serial number
show logging onboard message	Displays the hardware-related messages generated by a switch module
show logging onboard temperature	Displays the temperature of a switch module

These are examples of output from the show logging onboard commands:

```
Switch# show logging onboard clilog
--------------------------------------------------------------------------------
CLI LOGGING SUMMARY INFORMATION
--------------------------------------------------------------------------------
COUNT COMMAND
--------------------------------------------------------------------------------
    1 hw-module module logging onboard
    1 hw-module module logging onboard message level 7
    4 show logging onboard
    1 show logging onboard message
    1 show logging onboard summary
--------------------------------------------------------------------------------

Switch# show logging onboard temp
--------------------------------------------------------------------------------
TEMPERATURE SUMMARY INFORMATION
--------------------------------------------------------------------------------
Number of sensors          : 1
Sampling frequency         : 5 minutes
Maximum time of storage    : 720 minutes
--------------------------------------------------------------------------------
Sensor                              |   ID  | Maximum Temperature 0C
--------------------------------------------------------------------------------
System                                1     41
---------------------------------------
Temp                           Sensor ID
0C     1
---------------------------------------
No historical data to display
---------------------------------------

Switch# show logging onboard uptime
--------------------------------------------------------------------------------
UPTIME SUMMARY INFORMATION
--------------------------------------------------------------------------------
First customer power on : 03/01/1993 00:06:06
Total uptime            :   0 years  20 weeks   4 days   6 hours  20 minutes
Total downtime          :   0 years   0 weeks   0 days   0 hours   0 minutes
Number of resets        : 90
Number of slot changes  : 0
Current reset reason    : 0x0
Current reset timestamp : 03/01/1993 00:05:43
Current slot            : 1
Current uptime          :   0 years   0 weeks   2 days   6 hours   0 minutes
--------------------------------------------------------------------------------
Reset  |         |
Reason | Count   |
--------------------------------------------------------------------------------
No historical data to display
--------------------------------------------------------------------------------
```

```
Switch# show logging onboard voltage
-------------------------------------------------------------------------------------
VOLTAGE SUMMARY INFORMATION
-------------------------------------------------------------------------------------
Number of sensors          : 6
Sampling frequency         : 1 minutes
Maximum time of storage    : 720 minutes
-------------------------------------------------------------------------------------
Sensor                            |   ID  | Maximum Voltage
-------------------------------------------------------------------------------------
12.00V                              0      12.567
1.25V                               2       1.258
3.30V                               3       3.305
2.50V                               4       2.517
1.80V                               5       1.825
1.50V                               6       1.508
-------------------------------------------------------------------------------------
Nominal Range                         Sensor ID

-------------------------------------------------------------------------------------
No historical data to display
-------------------------------------------------------------------------------------
```

Initial Configuration with the CLI Setup Program

To set up the initial configuration for the switch module, you can use the CLI setup program, which runs automatically after the switch module powers on. You must assign an IP address and other configuration information necessary for the switch module to communicate with the local routers and the Internet.

Information You Need

Before you run the CLI Setup program, you need the following information:

- Switch Module IP address
- Subnet mask (IP netmask)
- Default gateway (router)
- Enable secret password
- Enable password
- Telnet password

Completing the Setup Program

Follow these steps to complete the setup program and to create an initial configuration for the switch module:

Step 1 Power up the CGR 2010 ESM.

The CLI Setup program runs automatically.

Step 2 Enter **Yes** at these two prompts.

```
Would you like to enter the initial configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system.

Would you like to enter basic management setup? [yes/no]: yes
```

Step 3 Enter a host name for the switch module, and press **Return**.

On a command switch module, the host name is limited to 28 characters and on a member switch module to 31 characters. Do not use *-n*, where *n* is a number, as the last character in a host name for any switch module.

```
Enter host name [Switch]: host_name
```

Step 4 Enter an enable secret password, and press **Return**.

The password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, allows spaces, but ignores leading spaces. The secret password is encrypted, and the enable password is in plain text.

```
Enter enable secret: secret_password
```

Step 5 Enter an enable password, and press **Return**.

```
Enter enable password: enable_password
```

Step 6 Enter a virtual terminal (Telnet) password, and press **Return**.

The password can be from 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores leading spaces.

```
Enter virtual terminal password: terminal-password
```

Step 7 (Optional) Configure Simple Network Management Protocol (SNMP) by responding to the prompts. You can also configure SNMP later through the CLI. To configure SNMP later, enter **no**.

```
Configure SNMP Network Management? [no]: no
```

Step 8 Enter the interface name (physical interface or VLAN name) of the interface that connects to the management network, and press **Return**. For this release, always use **vlan1** as that interface.

```
Enter interface name used to connect to the
management network from the above interface summary: vlan1
```

Step 9 Configure the interface by entering the switch module IP address and subnet mask and pressing **Return**. The IP address and subnet masks shown below are examples.

```
Configuring interface vlan1:
Configure IP on this interface? [yes]: yes
IP address for this interface: 10.4.120.106
Subnet mask for this interface [255.0.0.0]: 255.0.0.0
```

Step 10 Enter **Y** to configure the switch module as the cluster command switch module. Enter **N** to configure it as a member switch module or as a standalone switch module.

If you enter **N**, you can configure the switch module as a command switch module later through the CLI. To configure it later, enter **no**.

```
Would you like to enable as a cluster command switch? [yes/no]: no
```

You have completed the initial configuration of the switch module, and the switch module displays its configuration. This is an example of the configuration output:

```
The following configuration command script was created:
hostname switch1
enable secret 5 $1$Ulq8$DlA/OiaEbl90WcBPd9cOn1
enable password enable_password
line vty 0 15
password terminal-password
no snmp-server
!
no ip routing

!
interface Vlan1
no shutdown
ip address 10.4.120.106 255.0.0.0
!
interface FastEthernet1/0/1
!
interface FastEthernet1/0/2

interface FastEthernet1/0/3
!
...<output abbreviated>
end
```

Step 11 These choices appear:

```
[0] Go to the IOS command prompt without saving this config.

[1] Return back to the setup without saving this config.

[2] Save this configuration to nvram and exit.

If you want to save the configuration and use it the next time the switch module reboots,
select option 2 to save it in NVRAM.

Enter your selection [2]:2
```

Make your selection, and press **Return**.

After you complete the setup program, the switch module can run the default configuration that you created. To change this configuration or to perform other management tasks, enter commands at the `Switch>` prompt.

Cisco IOS File System, Configuration Files, and Software Images

This appendix describes how to manipulate the CGR 2010 ESM flash file system, how to copy configuration files, and how to archive (upload and download) software images to a switch module.

Note For complete syntax and usage information for the commands used in this chapter, see the switch module command reference for this release and the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*.

This appendix contains the following sections:

Working with the Flash File System

The flash file system is a single flash device on which you can store files. It also provides several commands to help you manage software image and configuration files. The default flash file system on the switch module is named *flash:*.

Unlike the Cisco CGS 2520 switch, the switch module does not have a removable SD flash memory card. The switch module stores images and configuration files in the internal flash. The internal flash is 64 MB, which is sufficient for holding several IOS images and all the necessary configuration files.

You can replace and upgrade the switch module without reconfiguring it. Use the **show flash:** privileged EXEC command to display the compact flash file settings. For more information about the command, go to this URL:

http://www.cisco.com/en/US/docs/ios/12_2/configfun/command/reference/frf009.html#wp1018357

Displaying Available File Systems

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

```
Switch# show file systems
File Systems:
     Size(b)     Free(b)      Type  Flags   Prefixes
*   15998976     5135872     flash     rw   flash:
           -           -    opaque     rw   bs:
           -           -    opaque     rw   vb:
      524288      520138     nvram     rw   nvram:
           -           -   network     rw   tftp:
           -           -    opaque     rw   null:
           -           -    opaque     rw   system:
           -           -    opaque     ro   xmodem:
           -           -    opaque     ro   ymodem:
```

Table B-1 Show File Systems Field Descriptions

Field	Value
Size(b)	Amount of memory in the file system in bytes
Free(b)	Amount of free memory in the file system in bytes
Type	Type of file system. **flash**—File system is for a flash memory device **nvram**—File system is for a NVRAM device **opaque**—File system is a locally generated *pseudo* file system (for example, the *system*) or a download interface, such as brimux **unknown**—File system is an unknown type

Table B-1 Show File Systems Field Descriptions (continued)

Field	Value
Flags	Permission for file system. **ro**—read-only **rw**—read/write **wo**—write-only
Prefixes	Alias for file system. **flash:**—Flash file system **nvram:**—NVRAM **null:**—Null destination for copies; you can copy a remote file to null to find its size **rcp:**—Remote Copy Protocol (RCP) network server **system:**—Contains the system memory, including the running configuration **tftp:**—TFTP network server **xmodem:**—Obtain the file from a network machine by using the Xmodem protocol **ymodem:**—Obtain the file from a network machine by using the Ymodem protocol

Setting the Default File System

You can specify the file system or directory that the system uses as the default file system by using the **cd** *filesystem:* privileged EXEC command. You can set the default file system to omit the *filesystem:* argument from related commands. For example, for all privileged EXEC commands that have the optional *filesystem:* argument, the system uses the file system specified by the **cd** command.

By default, the default file system is *flash:*.

You can display the current default file system as specified by the **cd** command by using the **pwd** privileged EXEC command.

Displaying Information about Files on a File System

You can view a list of the contents of a file system before manipulating its contents. For example, before copying a new configuration file to flash memory, you might want to verify that the file system does not already contain a configuration file with the same name. Similarly, before copying a flash configuration file to another location, you might want to verify its filename for use in another command.

To display information about files on a file system, use one of the privileged EXEC commands in Table B-2:

Table B-2 Commands for Displaying Information about Files

Command	Description
dir [**/all**] [*filesystem***:**][*filename*]	Display a list of files on a file system.
show file systems	Display more information about each of the files on a file system.

Table B-2 Commands for Displaying Information about Files (continued)

Command	Description
show file information *file-url*	Display information about a specific file.
show file descriptors	Display a list of open file descriptors. File descriptors are the internal representations of open files. You can use this command to see if another user has a file open.

Changing Directories and Displaying the Working Directory

Beginning in privileged EXEC mode, follow these steps to change directories and display the working directory.

	Step	Command
Step 1	Display the directories on the specified file system. For *filesystem***:**, use **flash:** for the system board flash device.	**dir** *filesystem***:**
Step 2	Change to the directory of interest. The command example shows how to change to the directory named *new_configs*.	**cd new_configs**
Step 3	Display the working directory.	**pwd**

Creating and Removing Directories

Beginning in privileged EXEC mode, follow these steps to create and remove a directory:

	Step	Command
Step 1	Display the directories on the specified file system. For *filesystem***:**, use **flash:** for the system board flash device.	**dir** *filesystem***:**
Step 2	Create a new directory. The command example shows how to create the directory named *old_configs*. Directory names are case sensitive. Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.	**mkdir old_configs**
Step 3	Verify your entry.	**dir** *filesystem***:**

To delete a directory with all its files and subdirectories, use the **delete /force /recursive** *filesystem***:/***file-url* privileged EXEC command.

Use the **/recursive** keyword to delete the named directory and all subdirectories and the files contained in it. Use the **/force** keyword to suppress the prompting that confirms a deletion of each file in the directory. You are prompted only once at the beginning of this deletion process. Use the **/force** and **/recursive** keywords for deleting old software images that were installed by using the **archive download-sw** command but are no longer needed.

For *filesystem*, use **flash:** for the system board flash device. For *file-url*, enter the name of the directory to be deleted. All the files in the directory and the directory are removed.

Caution When files and directories are deleted, their contents cannot be recovered.

Copying Files

To copy a file from a source to a destination, use the **copy** *source-url destination-url* privileged EXEC command. For the source and destination URLs, you can use **running-config** and **startup-config** keyword shortcuts. For example, the **copy running-config startup-config** command saves the currently running configuration file to the NVRAM section of flash memory to be used as the configuration during system initialization.

You can also copy from special file systems (**xmodem:**, **ymodem:**) as the source for the file from a network machine that uses the Xmodem or Ymodem protocol.

Network file system URLs include **ftp:**, **rcp:**, and **tftp:** and have these syntaxes:

- FTP—**ftp:**[[*//username* [**:***password*]*@location*]*/directory*]*/filename*
- RCP—**rcp:**[[*//username@location*]*/directory*]*/filename*
- TFTP—**tftp:**[[*//location*]*/directory*]*/filename*

In addition, the Secure Copy Protocol (SCP) provides a secure and authenticated method for copying switch module configurations or switch module image files. SCP relies on Secure Shell (SSH), an application and a protocol that provides a secure replacement for the Berkeley r-tools.

Note For more information on how to configure and verify SCP, see the "Secure Copy Protocol" chapter of the *Cisco IOS New Features, Cisco IOS Release 12.2T,* at this URL: http://www.cisco.com/en/US/docs/ios/12_2t/12_2t2/feature/guide/ftscp.html

Local writable file systems include flash:.

Some invalid combinations of source and destination exist. Specifically, you cannot copy these combinations:

- From a running configuration to a running configuration
- From a startup configuration to a startup configuration
- From a device to the same device (for example, the **copy flash: flash:** command is invalid)

For specific examples of using the **copy** command with configuration files, see the "Working with Configuration Files" section on page B-8.

To copy software images either by downloading a new version or by uploading the existing one, use the **archive download-sw** or the **archive upload-sw** privileged EXEC command. For more information, see the "Working with Software Images" section on page B-24.

Deleting Files

When you no longer need a file on a flash memory device, you can permanently delete it. To delete a file or directory from a specified flash device, use the **delete** [**/force**] [**/recursive**] [*filesystem***:**]*/file-url* privileged EXEC command.

Use the **/recursive** keyword for deleting a directory and all subdirectories and the files contained in it. Use the **/force** keyword to suppress the prompting that confirms a deletion of each file in the directory. You are prompted only once at the beginning of this deletion process. Use the **/force** and **/recursive** keywords for deleting old software images that were installed by using the **archive download-sw** command but are no longer needed.

If you omit the *filesystem***:** option, the switch module uses the default device specified by the **cd** command. For *file-url*, you specify the path (directory) and the name of the file to be deleted.

When you attempt to delete any files, the system prompts you to confirm the deletion.

Caution When files are deleted, their contents cannot be recovered.

This example shows how to delete the file *myconfig* from the default flash memory device:

```
Switch# delete myconfig
```

Creating, Displaying, and Extracting tar Files

You can create a tar file and write files into it, list the files in a tar file, and extract the files from a tar file as described in the next sections.

Note Instead of using the **copy** privileged EXEC command or the **archive tar** privileged EXEC command, we recommend using the **archive download-sw** and **archive upload-sw** privileged EXEC commands to download and upload software image files.

Creating a Tar File

To create a tar file and write files into it, use this privileged EXEC command:

archive tar /create *destination-url* **flash:***/file-url*

For *destination-url*, specify the destination URL alias for the local or network file system and the name of the tar file to create. These options are supported:

- For the local flash file system, the syntax is **flash:**
- For the FTP, the syntax is **ftp:**[[*//username*[**:***password*]*@location*]*/directory*]*/tar-filename***.tar**
- For the RCP, the syntax is **rcp:**[[*//username@location*]*/directory*]*/tar-filename***.tar**

- For the TFTP, the syntax is
  tftp:[[*//location*]*/directory*]*/tar-filename*.**tar**

The *tar-filename*.**tar** is the tar file to be created.

For **flash:/***file-url*, specify the location on the local flash file system from which the new tar file is created. You can also specify an optional list of files or directories within the source directory to write to the new tar file. If none are specified, all files and directories at this level are written to the newly created tar file.

This example shows how to create a tar file. This command writes the contents of the *new-configs* directory on the local flash device to a file named *saved.tar* on the TFTP server at 172.20.10.30:

```
Switch# archive tar /create tftp:172.20.10.30/saved.tar flash:/new-configs
```

Displaying the Contents of a tar File

To display the contents of a tar file on the screen, use this privileged EXEC command:

archive tar /table *source-url*

For *source-url*, specify the source URL alias for the local or network file system. These options are supported:

- For the local flash file system, the syntax is
  flash:
- For the FTP, the syntax is
  ftp:[[*//username*[**:***password*]*@location*]*/directory*]*/tar-filename*.**tar**
- For the RCP, the syntax is
  rcp:[[*//username@location*]*/directory*]*/tar-filename*.**tar**
- For the TFTP, the syntax is
  tftp:[[*//location*]*/directory*]*/tar-filename*.**tar**

The *tar-filename*.**tar** is the tar file to display.

This example shows how to display the contents of a switch module tar file that is in flash memory:

```
Switch# archive tar /table flash:image-name.tar
info (219 bytes)
image-name/ (directory)
image-name/html/ (directory)
image-name/html/foo.html (0 bytes)
image-name/image-name.bin (4527884 bytes)
image-name/info (346 bytes)
info (110 bytes)
```

Extracting a Tar File

To extract a tar file into a directory on the flash file system, use this privileged EXEC command:

archive tar /xtract *source-url* **flash:/***file-url* [*dir/file...*]

For *source-url*, specify the source URL alias for the local file system. These options are supported:

- For the local flash file system, the syntax is
  flash:
- For the FTP, the syntax is
  ftp:[[*//username*[**:***password*]*@location*]*/directory*]*/tar-filename*.**tar**

- For the RCP, the syntax is **rcp:**[[*//username@location*]*/directory*]*/tar-filename*.**tar**
- For the TFTP, the syntax is **tftp:**[[*//location*]*/directory*]*/tar-filename*.**tar**

The *tar-filename*.**tar** is the tar file from which to extract files.

For **flash:/***file-url* [*dir/file...*], specify *t*he location on the local flash file system into which the tar file is extracted. Use the *dir/file...* option to specify an optional list of files or directories within the tar file to be extracted. If none are specified, all files and directories are extracted.

This example shows how to extract the contents of a tar file located on the TFTP server at 172.20.10.30. This command extracts just the *new-configs* directory into the root directory on the local flash file system. The remaining files in the *saved.tar* file are ignored.

```
Switch# archive tar /xtract tftp://172.20.10.30/saved.tar flash:/new-configs
```

Displaying the Contents of a File

To display the contents of any readable file, including a file on a remote file system, use the **more** [**/ascii** | **/binary** | **/ebcdic**] *file-url* privileged EXEC command:.

This example shows how to display the contents of a configuration file on a TFTP server:

```
Switch# more tftp://serverA/hampton/savedconfig
!
! Saved configuration on server
!
version 11.3
service timestamps log datetime localtime
service linenumber
service udp-small-servers
service pt-vty-logging
!
<output truncated>
```

Working with Configuration Files

This section describes how to create, load, and maintain configuration files.

Configuration files contain commands entered to customize the function of the Cisco IOS software. A way to create a basic configuration file is to use the **setup** program or to enter the **setup** privileged EXEC command.

You can copy (*download*) configuration files from a TFTP, FTP, or RCP server to the running configuration or startup configuration of the switch module. You might want to perform this for one of these reasons:

- To restore a backed-up configuration file.
- To use the configuration file for another switch module. For example, you might add another switch module to your network and want it to have a configuration similar to the original switch module. By copying the file to the new switch module, you can change the relevant parts rather than recreating the whole file.
- To load the same configuration commands on all the switches in your network so that all the switches have similar configurations.

You can copy (*upload*) configuration files from the switch module to a file server by using TFTP, FTP, or RCP. You might perform this task to back up a current configuration file to a server before changing its contents so that you can later restore the original configuration file from the server.

The protocol you use depends on which type of server you are using. The FTP and RCP transport mechanisms provide faster performance and more reliable delivery of data than TFTP. These improvements are possible because FTP and RCP are built on and use the TCP/IP stack, which is connection-oriented.

These sections contain this configuration information:

Guidelines for Creating and Using Configuration Files

Creating configuration files can aid in your switch module configuration. Configuration files can contain some or all of the commands needed to configure one or more switches. For example, you might want to download the same configuration file to several switches that have the same hardware configuration.

Use these guidelines when creating a configuration file:

- We recommend that you connect through the host router's console port for the initial configuration of the switch module. If you are accessing the switch module through a network connection instead of through a connection to the router's console port, keep in mind that some configuration changes (such as changing the switch module IP address or disabling ports) can cause a loss of connectivity to the switch module. For details, see Chapter 3, "Accessing the Switch Module from the Host Router."
- If no password has been set on the switch module, we recommend that you set one by using the **enable secret** *secret-password* global configuration command.

Note The **copy** {**ftp: | rcp: | tftp:**} **system:running-config** privileged EXEC command loads the configuration files on the switch module as if you were entering the commands at the command line. The switch module does not erase the existing running configuration before adding the commands. If a command in the copied configuration file replaces a command in the existing configuration file, the existing command is erased.

For example, if the copied configuration file contains a different IP address in a particular command than the existing configuration, the IP address in the copied configuration is used. However, some commands in the existing configuration might not be replaced or negated. In this case, the resulting configuration file is a mixture of the existing configuration file and the copied configuration file, with the copied configuration file having precedence.

To restore a configuration file to an exact copy of a file stored on a server, copy the configuration file directly to the startup configuration (by using the **copy** {**ftp:** | **rcp:** | **tftp:**} **nvram:startup-config** privileged EXEC command), and reload the switch module.

Configuration File Types and Location

Startup configuration files are used during system startup to configure the software. Running configuration files contain the current configuration of the software. The two configuration files can be different. For example, you might want to change the configuration for a short time period rather than permanently. In this case, you would change the running configuration but not save the configuration by using the **copy running-config startup-config** privileged EXEC command.

The running configuration is saved in DRAM; the startup configuration is stored in the NVRAM section of flash memory.

Creating a Configuration File By Using a Text Editor

When creating a configuration file, you must list commands logically so that the system can respond appropriately. This is one method of creating a configuration file:

Step 1 Copy an existing configuration from a switch module to a server.

For more information, see the "Downloading the Configuration File By Using TFTP" section on page B-11, the "Downloading a Configuration File By Using FTP" section on page B-13, or the "Downloading a Configuration File By Using RCP" section on page B-17.

Step 2 Open the configuration file in a text editor, such as vi or emacs on UNIX or Notepad on a PC.

Step 3 Extract the portion of the configuration file with the desired commands, and save it in a new file.

Step 4 Copy the configuration file to the appropriate server location. For example, copy the file to the TFTP directory on the workstation (usually /tftpboot on a UNIX workstation).

Step 5 Make sure the permissions on the file are set to world-read.

Copying Configuration Files By Using TFTP

You can configure the switch module by using configuration files you create, download from another switch module, or download from a TFTP server. You can copy (upload) configuration files to a TFTP server for storage.

These sections contain this configuration information:

Preparing to Download or Upload a Configuration File By Using TFTP

Before you begin downloading or uploading a configuration file by using TFTP, do these tasks:

- Ensure that the workstation acting as the TFTP server is properly configured. On a Sun workstation, make sure that the /etc/inetd.conf file contains this line:

  ```
  tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
  ```

  Make sure that the /etc/services file contains this line:

  ```
  tftp 69/udp
  ```

  Note You must restart the inetd daemon after modifying the /etc/inetd.conf and /etc/services files. To restart the daemon, either stop the inetd process and restart it, or enter a **fastboot** command (on the SunOS 4.x) or a **reboot** command (on Solaris 2.x or SunOS 5.x). For more information on the TFTP daemon, see the documentation for your workstation.

- Ensure that the switch module has a route to the TFTP server. The switch module and the TFTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the TFTP server by using the **ping** command.
- Ensure that the configuration file to be downloaded is in the correct directory on the TFTP server (usually /tftpboot on a UNIX workstation).
- For download operations, ensure that the permissions on the file are set correctly. The permission on the file should be world-read.
- Before uploading the configuration file, you might need to create an empty file on the TFTP server. To create an empty file, enter the **touch** *filename* command, where *filename* is the name of the file you will use when uploading it to the server.
- During upload operations, if you are overwriting an existing file (including an empty file, if you had to create one) on the server, ensure that the permissions on the file are set correctly. Permissions on the file should be world-write.

Downloading the Configuration File By Using TFTP

To configure the switch module by using a configuration file downloaded from a TFTP server, follow these steps:

Step 1 Copy the configuration file to the appropriate TFTP directory on the workstation.

Step 2 Verify that the TFTP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File By Using TFTP" section on page B-11.

Step 3 Log into the switch module through the host router's console port or a Telnet session (for details, see Chapter 3, "Accessing the Switch Module from the Host Router."

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

Specify the IP address or hostname of the TFTP server and the name of the file to download.

Use one of these privileged EXEC commands:

- **copy tftp:**[[[*//location*]*/directory*]*/filename*] **system:running-config**
- **copy tftp:**[[[*//location*]*/directory*]*/filename*] **nvram:startup-config**

The configuration file downloads, and the commands are executed as the file is parsed line-by-line.

This example shows how to configure the software from the file *tokyo-confg* at IP address 172.16.2.155:

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

Uploading the Configuration File By Using TFTP

To upload a configuration file from a switch module to a TFTP server for storage, follow these steps:

Step 1 Verify that the TFTP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File By Using TFTP" section on page B-11.

Step 2 Log into the switch module through the host router's console port or a Telnet session (for details, see "Access the Switch Module from the Host Router").

Step 3 Upload the switch module configuration to the TFTP server. Specify the IP address or hostname of the TFTP server and the destination filename.

Use one of these privileged EXEC commands:

- **copy system:running-config tftp:**[[[*//location*]*/directory*]*/filename*]
- **copy nvram:startup-config tftp:**[[[*//location*]*/directory*]*/filename*]

The file is uploaded to the TFTP server.

This example shows how to upload a configuration file from a switch module to a TFTP server:

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

Copying Configuration Files By Using FTP

You can copy configuration files to or from an FTP server.

The FTP protocol requires a client to send a remote username and password on each FTP request to a server.

When you copy a configuration file from the switch module to a server by using FTP, the Cisco IOS software sends the first valid username in this list:

- The username specified in the **copy** command if a username is specified.
- The username set by the **ip ftp username** *username* global configuration command if the command is configured.
- Anonymous.

The switch module sends the first valid password in this list:

- The password specified in the **copy** command if a password is specified.

- The password set by the **ip ftp password** *password* global configuration command if the command is configured.
- The switch module forms a password named *username@switchname.domain*. The variable *username* is the username associated with the current session, *switchname* is the configured hostname, and *domain* is the domain of the switch module.

The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept your FTP write request.

Use the **ip ftp username** and **ip ftp password** commands to specify a username and password for all copies. Include the username in the **copy** command if you want to specify only a username for that copy operation.

If the server has a directory structure, the configuration file is written to or copied from the directory associated with the username on the server. For example, if the configuration file resides in the home directory of a user on the server, specify that user's name as the remote username.

For more information, see the documentation for your FTP server.

These sections contain this configuration information:

- Preparing to Download or Upload a Configuration File By Using FTP, page B-13
- Downloading a Configuration File By Using FTP, page B-13
- Uploading a Configuration File By Using FTP, page B-15

Preparing to Download or Upload a Configuration File By Using FTP

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

- Ensure that the switch module has a route to the FTP server. The switch module and the FTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the FTP server by using the **ping** command.
- If you are accessing the switch module through the host router's console or a Telnet session and you do not have a valid username, make sure that the current FTP username is the one that you want to use for the FTP download. To view the valid username, you can enter the **show users** privileged EXEC command. If you do not want to use this username, create a new FTP username by using the **ip ftp username** *username* global configuration command during all copy operations. The new username is stored in NVRAM.

  If you are accessing the switch module through a Telnet session and you have a valid username, this username is used, and you do not need to set the FTP username. Include the username in the **copy** command if you want to specify a username for only that copy operation.
- When you upload a configuration file to the FTP server, it must be properly configured to accept the write request from the user on the switch module.

For more information, see the documentation for your FTP server.

Downloading a Configuration File By Using FTP

Beginning in privileged EXEC mode, follow these steps to download a configuration file by using FTP:

	Step	Command
Step 1	Verify that the FTP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File By Using FTP" section on page B-13.	
Step 2	Log into the switch module through the host router's console port or a Telnet session.	
Step 3	Enter global configuration mode on the switch module. This step is required only if you override the default remote username or password (see Steps 4, 5, and 6).	**configure terminal**
Step 4	(Optional) Change the default remote username.	**ip ftp username** *username*
Step 5	(Optional) Change the default password.	**ip ftp password** *password*
Step 6	Return to privileged EXEC mode.	**end**
Step 7	Using FTP, copy the configuration file from a network server to the running configuration or to the startup configuration file.	**copy ftp:**[[[**//**[*username*[**:***password*]@]*location*]**/***directory*]**/***filename*] **system:running-config** or **copy ftp:**[[[**//**[*username*[**:***password*]@]*location*]**/***directory*]**/***filename*] **nvram:startup-config**

This example shows how to copy a configuration file named *host1-confg* from the *netadmin1* directory on the remote server with an IP address of 172.16.101.101 and to load and run those commands on the switch module:

```
Switch# copy ftp://netadmin1:mypass@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
Switch#
%SYS-5-CONFIG: Configured from host1-config by ftp from 172.16.101.101
```

This example shows how to specify a remote username of *netadmin1*. The software copies the configuration file *host2-confg* from the *netadmin1* directory on the remote server with an IP address of 172.16.101.101 to the switch module startup configuration.

```
Switch# configure terminal
Switch(config)# ip ftp username netadmin1
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# copy ftp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
Switch#
```

```
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by ftp from
172.16.101.101
```

Uploading a Configuration File By Using FTP

Beginning in privileged EXEC mode, follow these steps to upload a configuration file by using FTP:

	Step	Command
Step 1	Verify that the FTP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File By Using FTP" section on page B-13.	
Step 2	Log into the switch module through the host router's console port or a Telnet session.	
Step 3	Enter global configuration mode. This step is required only if you override the default remote username or password (see Steps 4, 5, and 6).	**configure terminal**
Step 4	(Optional) Change the default remote username.	**ip ftp username** *username*
Step 5	(Optional) Change the default password.	**ip ftp password** *password*
Step 6	Return to privileged EXEC mode.	**end**
Step 7	Using FTP, store the switch module running or startup configuration file to the specified location.	**copy system:running-config ftp:**[[[**//**[*username*[**:***password*]**@**]*location*]**/***directory*]**/***filename*] or **copy nvram:startup-config ftp:**[[[**//**[*username*[**:***password*]**@**]*location*]**/***directory*]**/***filename*]

This example shows how to copy the running configuration file named *switch2-confg* to the *netadmin1* directory on the remote host with an IP address of 172.16.101.101:

```
Switch# copy system:running-config ftp://netadmin1:mypass@172.16.101.101/switch2-confg
Write file switch2-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Switch#
```

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

```
Switch# configure terminal
Switch(config)# ip ftp username netadmin2
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# copy nvram:startup-config ftp:
Remote host[]? 172.16.101.101
Name of configuration file to write [switch2-confg]?
Write file switch2-confg on host 172.16.101.101?[confirm]
![OK]
```

Copying Configuration Files By Using RCP

The Remote Copy Protocol (RCP) provides another method of downloading, uploading, and copying configuration files between remote hosts and the switch module. Unlike TFTP, which uses User Datagram Protocol (UDP), a connectionless protocol, RCP uses TCP, which is connection-oriented.

To use RCP to copy files, the server from or to which you will be copying files must support RCP. The RCP copy commands rely on the rsh server (or daemon) on the remote system. To copy files by using RCP, you do not need to create a server for file distribution as you do with TFTP. You only need to have access to a server that supports the remote shell (rsh). (Most UNIX systems support rsh.) Because you are copying a file from one place to another, you must have read permission on the source file and write permission on the destination file. If the destination file does not exist, RCP creates it for you.

The RCP requires a client to send a remote username with each RCP request to a server. When you copy a configuration file from the switch module to a server, the Cisco IOS software sends the first valid username in this list:

- The username specified in the **copy** command if a username is specified.
- The username set by the **ip rcmd remote-username** *username* global configuration command if the command is configured.
- The remote username associated with the current TTY (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the **username** command, the switch module software sends the Telnet username as the remote username.
- The switch module hostname.

For a successful RCP copy request, you must define an account on the network server for the remote username. If the server has a directory structure, the configuration file is written to or copied from the directory associated with the remote username on the server. For example, if the configuration file is in the home directory of a user on the server, specify that user's name as the remote username.

These sections contain this configuration information:

- Preparing to Download or Upload a Configuration File By Using RCP, page B-16
- Downloading a Configuration File By Using RCP, page B-17
- Uploading a Configuration File By Using RCP, page B-18

Preparing to Download or Upload a Configuration File By Using RCP

Before you begin downloading or uploading a configuration file by using RCP, do these tasks:

- Ensure that the workstation acting as the RCP server supports the remote shell (rsh).
- Ensure that the switch module has a route to the RCP server. The switch module and the server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the RCP server by using the **ping** command.
- If you are accessing the switch module through the host router's console or a Telnet session and you do not have a valid username, make sure that the current RCP username is the one that you want to use for the RCP download.
- To view the valid username, you can enter the **show users** privileged EXEC command. If you do not want to use this username, create a new RCP username by using the **ip rcmd remote-username** *username* global configuration command to be used during all copy operations. The new username is stored in NVRAM.

- If you are accessing the switch module through a Telnet session and you have a valid username, this username is used, and you do not need to set the RCP username. Include the username in the **copy** command if you want to specify a username for only that copy operation.
- When you upload a file to the RCP server, it must be properly configured to accept the RCP write request from the user on the switch module. For UNIX systems, you must add an entry to the .rhosts file for the remote user on the RCP server. For example, suppose that the switch module contains these configuration lines:

```
hostname Switch1
ip rcmd remote-username User0
```

If the switch module IP address translates to *Switch1.company.com*, the .rhosts file for User0 on the RCP server should contain this line:

```
Switch1.company.com Switch1
```

For more information, see the documentation for your RCP server.

Downloading a Configuration File By Using RCP

Beginning in privileged EXEC mode, follow these steps to download a configuration file by using RCP:

	Step	Command
Step 1	Verify that the RCP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File By Using RCP" section on page B-16.	
Step 2	Log into the switch module through the host router's console port or a Telnet session.	
Step 3	Enter global configuration mode. This step is required only if you override the default remote username (see Steps 4 and 5).	**configure terminal**
Step 4	(Optional) Specify the remote username.	**ip rcmd remote-username** *username*
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Using RCP, copy the configuration file from a network server to the running configuration or to the startup configuration file.	**copy rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*] **system:running-config** or **copy rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*] **nvram:startup-config**

This example shows how to copy a configuration file named *host1-confg* from the *netadmin1* directory on the remote server with an IP address of 172.16.101.101 and load and run those commands on the switch module:

```
Switch# copy rcp://netadmin1@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
```

```
Switch#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

This example shows how to specify a remote username of *netadmin1*. Then it copies the configuration file *host2-confg* from the *netadmin1* directory on the remote server with an IP address of 172.16.101.101 to the startup configuration:

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin1
Switch(config)# end
Switch# copy rcp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
Switch#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by rcp from
172.16.101.101
```

Uploading a Configuration File By Using RCP

Beginning in privileged EXEC mode, follow these steps to upload a configuration file by using RCP:

	Step	Command
Step 1	Verify that the RCP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File By Using RCP" section on page B-16.	
Step 2	Log into the switch module through the host router's console port or a Telnet session.	
Step 3	Enter global configuration mode. This step is required only if you override the default remote username (see Steps 4 and 5).	**configure terminal**
Step 4	(Optional) Specify the remote username.	**ip rcmd remote-username** *username*
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Using RCP, copy the configuration file from a switch module running or startup configuration file to a network server.	**copy system:running-config rcp:**[[[**//**[*username*@]*location*]/*directory*]/*filename*] or **copy nvram:startup-config rcp:**[[[**//**[*username*@]*location*]/*directory*]/*filename*]

This example shows how to copy the running configuration file named *switch2-confg* to the *netadmin1* directory on the remote host with an IP address of 172.16.101.101:

```
Switch# copy system:running-config rcp://netadmin1@172.16.101.101/switch2-confg
Write file switch-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Switch#
```

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

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin2
Switch(config)# end
Switch# copy nvram:startup-config rcp:
Remote host[]? 172.16.101.101
Name of configuration file to write [switch2-confg]?
Write file switch2-confg on host 172.16.101.101?[confirm]
![OK]
```

Clearing Configuration Information

You can clear the configuration information from the startup configuration. If you reboot the switch module with no startup configuration, the switch module enters the setup program so that you can reconfigure the switch module with all new settings.

Clearing the Startup Configuration File

To clear the contents of your startup configuration, use the **erase nvram:** or the **erase startup-config** privileged EXEC command.

Caution You cannot restore the startup configuration file after it has been deleted.

Deleting a Stored Configuration File

To delete a saved configuration from flash memory, use the **delete flash:***filename* privileged EXEC command. Depending on the setting of the **file prompt** global configuration command, you might be prompted for confirmation before you delete a file. By default, the switch module prompts for confirmation on destructive file operations. For more information about the **file prompt** command, see the *Cisco IOS Command Reference for Release 12.2*.

Caution You cannot restore a file after it has been deleted.

Replacing and Rolling Back Configurations

The configuration replacement and rollback feature replaces the running configuration with any saved Cisco IOS configuration file. You can use the rollback function to roll back to a previous configuration.

These sections contain this information:

Understanding Configuration Replacement and Rollback

Archiving a Configuration

The configuration archive provides a mechanism to store, organize, and manage an archive of configuration files. The **configure replace** privileged EXEC command increases the configuration rollback capability. As an alternative, you can save copies of the running configuration by using the **copy running-config** *destination-url* privileged EXEC command, storing the replacement file either locally or remotely. However, this method lacks any automated file management. The configuration replacement and rollback feature can automatically save copies of the running configuration to the configuration archive.

You use the **archive config** privileged EXEC command to save configurations in the configuration archive by using a standard location and filename prefix that is automatically appended with an incremental version number (and optional timestamp) as each consecutive file is saved. You can specify how many versions of the running configuration are kept in the archive. After the maximum number of files are saved, the oldest file is automatically deleted when the next, most recent file is saved. The **show archive** privileged EXEC command displays information for all the configuration files saved in the configuration archive.

The Cisco IOS configuration archive, in which the configuration files are stored and available for use with the **configure replace** command, is in any of these file systems: FTP, HTTP, RCP, TFTP.

Replacing a Configuration

The **configure replace** privileged EXEC command replaces the running configuration with any saved configuration file. When you enter the **configure replace** command, the running configuration is compared with the specified replacement configuration, and a set of configuration differences is generated. The resulting differences are used to replace the configuration. The configuration replacement operation is usually completed in no more than three passes. To prevent looping behavior no more than five passes are performed.

You can use the **copy** *source-url* **running-config** privileged EXEC command to copy a stored configuration file to the running configuration. When using this command as an alternative to the **configure replace** *target-url* privileged EXEC command, note these major differences:

- The **copy** *source-url* **running-config** command is a merge operation and preserves all the commands from both the source file and the running configuration. This command does not remove commands from the running configuration that are not present in the source file. In contrast, the **configure replace** *target-url* command removes commands from the running configuration that are not present in the replacement file and adds commands to the running configuration that are not present.
- You can use a partial configuration file as the source file for the **copy** *source-url* **running-config** command. You must use a complete configuration file as the replacement file for the **configure replace** *target-url* command.

Rolling Back a Configuration

You can also use the **configure replace** command to roll back changes that were made since the previous configuration was saved. Instead of basing the rollback operation on a specific set of changes that were applied, the configuration rollback capability reverts to a specific configuration based on a saved configuration file.

If you want the configuration rollback capability, you must first save the running configuration before making any configuration changes. Then, after entering configuration changes, you can use that saved configuration file to roll back the changes by using the **configure replace** *target-url* command.

You can specify any saved configuration file as the rollback configuration. You are not limited to a fixed number of rollbacks, as is the case in some rollback models.

Configuration Replacement and Rollback Guidelines

- Make sure that the switch module has free memory larger than the combined size of the two configuration files (the running configuration and the saved replacement configuration). Otherwise, the configuration replacement operation fails.
- Make sure that the switch module also has sufficient free memory to execute the configuration replacement or rollback configuration commands.
- Certain configuration commands, such as those pertaining to physical components of a networking device (for example, physical interfaces), cannot be added or removed from the running configuration.
  - A configuration replacement operation cannot remove the **interface** *interface-id* command line from the running configuration if that interface is physically present on the device.
  - The **interface** *interface-id* command line cannot be added to the running configuration if no such interface is physically present on the device.
- When using the **configure replace** command, you must specify a saved configuration as the replacement configuration file for the running configuration. The replacement file must be a complete configuration generated by a Cisco IOS device (for example, a configuration generated by the **copy running-config** *destination-url* command).

Note If you generate the replacement configuration file externally, it must comply with the format of files generated by Cisco IOS devices.

Configuring the Configuration Archive

Using the **configure replace** command with the configuration archive and with the **archive config** command is optional but offers significant benefit for configuration rollback scenarios. Before using the **archive config command**, you must first configure the configuration archive. Starting in privileged EXEC mode, follow these steps to configure the configuration archive:

	Step	Command
Step 1	Enter global configuration mode.	**configure terminal**
Step 2	Enter archive configuration mode.	**archive**
Step 3	Specify the location and filename prefix for the files in the configuration archive.	**path** *url*

	Step	Command
Step 4	(Optional) Set the maximum number of archive files of the running configuration to be saved in the configuration archive. *number*—Maximum files of the running configuration file in the configuration archive. Valid values are from 1 to 14. The default is 10. **Note** Before using this command, you must first enter the **path** archive configuration command to specify the location and filename prefix for the files in the configuration archive.	**maximum** *number*
Step 5	(Optional) Set the time increment for automatically saving an archive file of the running configuration in the configuration archive. *minutes*—Specify how often, in minutes, to automatically save an archive file of the running configuration in the configuration archive.	**time-period** *minutes*
Step 6	Return to privileged EXEC mode.	**end**
Step 7	Verify the configuration.	**show running-config**
Step 8	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

Performing a Configuration Replacement or Rollback Operation

Beginning in privileged EXEC mode, follow these steps to replace the running configuration file with a saved configuration file:

	Step	Command
Step 1	(Optional) Save the running configuration file to the configuration archive. **Note** Enter the **path** archive configuration command before using this command.	**archive config**
Step 2	Enter global configuration mode.	**configure terminal**
Step 3	Make necessary changes to the running configuration.	
Step 4	Return to privileged EXEC mode.	**exit**

	Step	Command
Step 5	Replace the running configuration file with a saved configuration file. *target-url*—URL (accessible by the file system) of the saved configuration file that is to replace the running configuration, such as the configuration file created in Step 2 by using the **archive config** privileged EXEC command. **list**—Display a list of the command entries applied by the software parser during each pass of the configuration replacement operation. The total number of passes also appears. **force**— Replace the running configuration file with the specified saved configuration file without prompting you for confirmation. **time** *seconds*—Specify the time (in seconds) within which you must enter the **configure confirm** command to confirm replacement of the running configuration file. If you do not enter the **configure confirm** command within the specified time limit, the configuration replacement operation is automatically stopped. (In other words, the running configuration file is restored to the configuration that existed before you entered the **configure replace** command). **Note** You must first enable the configuration archive before you can use the **time** *seconds* command line option. **nolock**—Disable the locking of the running configuration file that prevents other users from changing the running configuration during a configuration replacement operation.	**configure replace** *target-url* [**list**] [**force**] [**time** *seconds*] [**nolock**]
Step 6	(Optional) Confirm replacement of the running configuration with a saved configuration file. **Note** Use this command only if the **time** *seconds* keyword and argument of the **configure replace** command are specified.	**configure confirm**
Step 7	(Optional) Save your entries in the configuration file.	**copy running-config startup-config**

Working with Software Images

This section describes how to archive (download and upload) software image files, which contain the system software, the Cisco IOS code, and the embedded device manager software.

Note Instead of using the **copy** privileged EXEC command or the **archive tar** privileged EXEC command, we recommend using the **archive download-sw** and **archive upload-sw** privileged EXEC commands to download and upload software image files.

You can download a switch module image file from a TFTP, FTP, or RCP server to upgrade the switch module software.

You can replace the current image with the new one or keep the current image in flash memory after a download.

You upload a switch module image file to a TFTP, FTP, or RCP server for backup purposes. You can use this uploaded image for future downloads to the same switch module or to another of the same type.

The protocol that you use depends on which type of server you are using. The FTP and RCP transport mechanisms provide faster performance and more reliable delivery of data than TFTP. These improvements are possible because FTP and RCP are built on and use the TCP/IP stack, which is connection-oriented.

These sections contain this configuration information:

- Image Location on the Switch Module, page B-24
- Tar File Format of Images on a Server or Cisco.com, page B-25
- Copying Image Files By Using TFTP, page B-26
- Copying Image Files By Using FTP, page B-29
- Copying Image Files By Using RCP, page B-34

Note For a list of software images and the supported upgrade paths, see the release notes for your switch module.

Image Location on the Switch Module

The Cisco IOS image is stored as a *.bin* file in a directory that shows the version number. A subdirectory contains the files needed for web management. The image is stored on the system board flash memory (flash:).

You can use the **show version** privileged EXEC command to see the software version that is currently running on your switch module. In the display, check the line that begins with `System image file is...` . It shows the directory name in flash memory where the image is stored.

You can also use the **dir** *filesystem***:** privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

Tar File Format of Images on a Server or Cisco.com

Software images located on a server or downloaded from Cisco.com are provided in a tar file format, which contains these files:

- An *info* file, which serves as a table of contents for the tar file
- One or more subdirectories containing other images and files, such as Cisco IOS images

This example shows some of the information contained in the info file. Table B-3 provides additional details about this information:

```
version_suffix: image-name
version_directory: image-name
image_system_type_id: 0x00000000
image_name: image-name .bin
ios_image_file_size: 4526592
total_image_file_size: 4526592
image_feature: LAYER_2|MIN_DRAM_MEG=64
image_family: family
stacking_number: 1.11
board_ids: 0x00000029
info_end:
```

Note Disregard the stacking_number field. It does not apply to the switch module.

Table B-3 Info File Descriptions

Field	Description
version_suffix	Specifies the Cisco IOS image version string suffix
version_directory	Specifies the directory where the Cisco IOS image and the HTML subdirectory are installed
image_name	Specifies the name of the Cisco IOS image within the tar file
ios_image_file_size	Specifies the Cisco IOS image size in the tar file, which is an approximate measure of how much flash memory is required to hold just the Cisco IOS image
total_image_file_size	Specifies the size of all the images (the Cisco IOS image and the web management files) in the tar file, which is an approximate measure of how much flash memory is required to hold them
image_feature	Describes the core functionality of the image
image_min_dram	Specifies the minimum amount of DRAM needed to run this image
image_family	Describes the family of products on which the software can be installed

Copying Image Files By Using TFTP

You can download a switch module image from a TFTP server or upload the image from the switch module to a TFTP server.

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

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

Note Instead of using the **copy** privileged EXEC command or the **archive tar** privileged EXEC command, we recommend using the **archive download-sw** and **archive upload-sw** privileged EXEC commands to download and upload software image files.

These sections contain this configuration information:

- Preparing to Download or Upload an Image File By Using TFTP, page B-26
- Downloading an Image File By Using TFTP, page B-27
- Uploading an Image File By Using TFTP, page B-28

Preparing to Download or Upload an Image File By Using TFTP

Before you begin downloading or uploading an image file by using TFTP, do these tasks:

- Ensure that the workstation acting as the TFTP server is properly configured. On a Sun workstation, make sure that the /etc/inetd.conf file contains this line:

  ```
  tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
  ```

  Make sure that the /etc/services file contains this line:

  ```
  tftp 69/udp
  ```

  Note You must restart the inetd daemon after modifying the /etc/inetd.conf and /etc/services files. To restart the daemon, either stop the inetd process and restart it, or enter a **fastboot** command (on the SunOS 4.x) or a **reboot** command (on Solaris 2.x or SunOS 5.x). For more information on the TFTP daemon, see the documentation for your workstation.

- Ensure that the switch module has a route to the TFTP server. The switch module and the TFTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the TFTP server by using the **ping** command.
- Ensure that the image to be downloaded is in the correct directory on the TFTP server (usually /tftpboot on a UNIX workstation).
- For download operations, ensure that the permissions on the file are set correctly. The permission on the file should be world-read.
- Before uploading the image file, you might need to create an empty file on the TFTP server. To create an empty file, enter the **touch** *filename* command, where *filename* is the name of the file you will use when uploading the image to the server.

- During upload operations, if you are overwriting an existing file (including an empty file, if you had to create one) on the server, ensure that the permissions on the file are set correctly. Permissions on the file should be world-write.

Downloading an Image File By Using TFTP

You can download a new image file and replace the current image or keep the current image.

Beginning in privileged EXEC mode, follow Steps 1 through 3 to download a new image from a TFTP server and overwrite the existing image. To keep the current image, go to Step 4.

	Step	Command
Step 1	Copy the image to the appropriate TFTP directory on the workstation. Make sure the TFTP server is properly configured; see the "Preparing to Download or Upload an Image File By Using TFTP" section on page B-26.	
Step 2	Log into the switch module through the host router's console port or a Telnet session.	
Step 3	Download the image file from the TFTP server to the switch module, and overwrite the current image. • The **/overwrite** option overwrites the software image in flash memory with the downloaded image. • For **//***location*, specify the IP address of the TFTP server. • For */directory/image-name***.tar**, specify the directory and the image to download. Directory and image names are case sensitive.	**archive download-sw /overwrite tftp://***location/directory/image-name***.tar**
Step 4	Download the image file from the TFTP server to the switch module, and keep the current image. • The **/leave-old-sw** option keeps the old software version after a download. • For **//***location*, specify the IP address of the TFTP server. • For */directory/image-name***.tar**, specify the directory and the image to download. Directory and image names are case sensitive.	**archive download-sw /leave-old-sw tftp://***location/directory/image-name***.tar**
Step 5	After the download and untarring are completed, power cycle the CGR2010.	

The **archive download-sw** command untars/unzips the file. The system prompts you when it completes successfully. The download algorithm verifies that the image is appropriate for the switch module model and that enough DRAM is present, or it aborts the process and reports an error. If you specify the **/overwrite** option, the download algorithm removes the existing image on the flash device whether or not it is the same as the new one and downloads the new image.

If you specify the command without the **/overwrite** option, the download algorithm verifies that the new image is not the same as the one on the switch Flash device. If the images are the same, the download does not occur. If the images are different, the old image is deleted, and the new one is downloaded. If there is not enough space to install the new image and keep the current running image, the download process stops, and an error message is displayed.

Note If the flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the **/overwrite** option.

If you specify the **/leave-old-sw**, the existing files are not removed. If there is not enough space to install the new image and keep the current running image, the download process stops, and an error message is displayed.

The algorithm installs the downloaded image on the system board flash device (flash:). The image is placed into a new directory named with the software version string, and the BOOT environment variable is updated to point to the newly installed image.

If you kept the old image during the download process (you specified the **/leave-old-sw** keyword), you can remove it by entering the **delete /force /recursive** *filesystem***:/***file-url* privileged EXEC command. For *filesystem*, use **flash:** for the system board flash device. For *file-url*, enter the directory name of the old image. All the files in the directory and the directory are removed.

Caution For the download and upload algorithms to operate properly, do *not* rename image names.

Uploading an Image File By Using TFTP

You can upload an image from the switch module to a TFTP server. You can later download this image to the switch module or to another switch module of the same type.

Use the upload feature only if the web management pages associated with the embedded device manager have been installed with the existing image.

Beginning in privileged EXEC mode, follow these steps to upload an image to a TFTP server:

	Step	Command
Step 1	Make sure the TFTP server is properly configured; see the "Preparing to Download or Upload an Image File By Using TFTP" section on page B-26.	

	Step	Command
Step 2	Log into the switch module through the host router's console port or a Telnet session.	
Step 3	Upload the currently running switch module image to the TFTP server. • For **//***location*, specify the IP address of the TFTP server. • For **/***directory***/***image-name***.tar**, specify the directory and the name of the software image to be uploaded. Directory and image names are case sensitive. The *image-name***.tar** is the name of the software image to be stored on the server.	**archive upload-sw tftp://***location***/***directory***/***image-name***.tar**

The **archive upload-sw** privileged EXEC command builds an image file on the server by uploading these files in order: info, the Cisco IOS image, and the web management files. After these files are uploaded, the upload algorithm creates the tar file format.

Caution For the download and upload algorithms to operate properly, do *not* rename image names.

Copying Image Files By Using FTP

You can download a switch module image from an FTP server or upload the image from the switch module to an FTP server.

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

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

Note Instead of using the **copy** privileged EXEC command or the **archive tar** privileged EXEC command, we recommend using the **archive download-sw** and **archive upload-sw** privileged EXEC commands to download and upload software image files.

These sections contain this configuration information:

- Preparing to Download or Upload an Image File By Using FTP, page B-29
- Downloading an Image File By Using FTP, page B-31
- Uploading an Image File By Using FTP, page B-33

Preparing to Download or Upload an Image File By Using FTP

You can copy images files to or from an FTP server.

The FTP protocol requires a client to send a remote username and password on each FTP request to a server. When you copy an image file from the switch module to a server by using FTP, the Cisco IOS software sends the first valid username in this list:

- Username specified in the **archive download-sw** or **archive upload-sw** privileged EXEC command if a username is specified
- Username set by the **ip ftp username** *username* global configuration command if the command is configured
- Anonymous

The switch module sends the first valid password in this list:

- Password specified in the **archive download-sw** or **archive upload-sw** privileged EXEC command if a password is specified
- Password set by the **ip ftp password** *password* global configuration command if the command is configured
- Switch module forms a password named *username@switchname.domain*. The variable *username* is the username associated with the current session, *switchname* is the configured hostname, and *domain* is the domain of the switch module.

The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from you.

Use the **ip ftp username** and **ip ftp password** commands to specify a username and password for all copies. Include the username in the **archive download-sw** or **archive upload-sw** privileged EXEC command if you want to specify a username only for that operation.

If the server has a directory structure, the image file is written to or copied from the directory associated with the username on the server. For example, if the image file resides in the home directory of a user on the server, specify that user's name as the remote username.

Before you begin downloading or uploading an image file by using FTP, do these tasks:

- Ensure that the switch module has a route to the FTP server. The switch module and the FTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the FTP server by using the **ping** command.
- If you are accessing the switch module through the host router's console or a Telnet session and you do not have a valid username, make sure that the current FTP username is the one that you want to use for the FTP download.
- To view the valid username, you can enter the **show users** privileged EXEC command. If you do not want to use this username, create a new FTP username by using the **ip ftp username** *username* global configuration command. This new name will be used during all archive operations. The new username is stored in NVRAM. If you are accessing the switch module through a Telnet session and you have a valid username, this username is used, and you do not need to set the FTP username. Include the username in the **archive download-sw** or **archive upload-sw** privileged EXEC command if you want to specify a username for that operation only.
- When you upload an image file to the FTP server, it must be properly configured to accept the write request from the user on the switch module.

For more information, see the documentation for your FTP server.

Downloading an Image File By Using FTP

You can download a new image file and overwrite the current image or keep the current image.

Beginning in privileged EXEC mode, follow Steps 1 through 7 to download a new image from an FTP server and overwrite the existing image. To keep the current image, go to Step 8.

	Step	Command
Step 1	Verify that the FTP server is properly configured by referring to the "Preparing to Download or Upload an Image File By Using FTP" section on page B-29.	
Step 2	Log into the switch module through the host router's console port or a Telnet session.	
Step 3	Enter global configuration mode. This step is required only if you override the default remote username or password (see Steps 4, 5, and 6).	**configure terminal**
Step 4	(Optional) Change the default remote username.	**ip ftp username** *username*
Step 5	(Optional) Change the default password.	**ip ftp password** *password*
Step 6	Return to privileged EXEC mode.	**end**
Step 7	Download the image file from the FTP server to the switch module, and overwrite the current image. • The **/overwrite** option overwrites the software image in flash memory with the downloaded image. • For **//***username***:***password*, specify the username and password; these must be associated with an account on the FTP server. For more information, see the "Preparing to Download or Upload an Image File By Using FTP" section on page B-29. • For @*location*, specify the IP address of the FTP server • For *directory*/*image-name***.tar**, specify the directory and the image to download. Directory and image names are case sensitive.	**archive download-sw /overwrite ftp:** **//***username***:***password*@*location*/*directory*/*image-name***.tar**

	Step	Command
Step 8	Download the image file from the FTP server to the switch module, and keep the current image. • The **/leave-old-sw** option keeps the old software version after a download. • For **//***username***:***password*, specify the username and password. These must be associated with an account on the FTP server. For more information, see the "Preparing to Download or Upload an Image File By Using FTP" section on page B-29. • For **@***location*, specify the IP address of the FTP server. • For *directory*/*image-name*.**tar**, specify the directory and the image to download. Directory and image names are case sensitive.	**archive download-sw /leave-old-sw ftp://***username***:***password***@***location*/*directory*/*image-name*.tar**
Step 9	After the download and untarring complete, power cycle the CGR2010.	

The **archive download-sw** command untars/unzips the file. The system prompts you when it completes successfully. The download algorithm verifies that the image is appropriate for the switch module model and that enough DRAM is present, or it aborts the process and reports an error. If you specify the **/overwrite** option, the download algorithm removes the existing image on the flash device whether or not it is the same as the new one and downloads the new image.

If you specify the command without the **/overwrite** option, the download algorithm verifies that the new image is not the same as the one on the switch Flash device. If the images are the same, the download does not occur. If the images are different, the old image is deleted, and the new one is downloaded. If there is not enough space to install the new image and keep the current running image, the download process stops, and the system displays an error message.

Note If the flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the **/overwrite** option.

If you specify the **/leave-old-sw**, the existing files are not removed. If there is not enough space to install the new image and keep the running image, the download process stops, and an error message is displayed.

The algorithm installs the downloaded image onto the system board flash device (flash:). The image is placed into a new directory named with the software version string, and the BOOT environment variable is updated to point to the newly installed image.

If you kept the old image during the download process (you specified the **/leave-old-sw** keyword), you can remove it by entering the **delete /force /recursive** *filesystem***:/***file-url* privileged EXEC command. For *filesystem*, use **flash:** for the system board flash device. For *file-url*, enter the directory name of the old software image. All the files in the directory and the directory are removed.

Caution For the download and upload algorithms to operate properly, do *not* rename image names.

Uploading an Image File By Using FTP

You can upload an image from the switch module to an FTP server. You can later download this image to the same switch module or to another switch module of the same type.

Use the upload feature only if the web management pages associated with the embedded device manager have been installed with the existing image.

Beginning in privileged EXEC mode, follow these steps to upload an image to an FTP server:

	Step	Command
Step 1	Verify that the FTP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File By Using FTP" section on page B-13.	
Step 2	Log into the switch module through the host router's console port or a Telnet session.	
Step 3	Enter global configuration mode. This step is required only if you override the default remote username or password (see Steps 4, 5, and 6).	**configure terminal**
Step 4	(Optional) Change the default remote username.	**ip ftp username** *username*
Step 5	(Optional) Change the default password.	**ip ftp password** *password*
Step 6	Return to privileged EXEC mode.	**end**
Step 7	Upload the currently running switch module image to the FTP server. • For **//***username***:***password*, specify the username and password. These must be associated with an account on the FTP server. For more information, see the "Preparing to Download or Upload an Image File By Using FTP" section on page B-29. • For @*location*, specify the IP address of the FTP server. • For **/***directory***/***image-name***.tar**, specify the directory and the name of the software image to be uploaded. Directory and image names are case sensitive. The *image-name***.tar** is the name of the software image to be stored on the server.	**archive upload-sw ftp://***username***:***password***@***location***/***directory***/***image-name***.tar**

The **archive upload-sw** command builds an image file on the server by uploading these files in order: info, the Cisco IOS image, and the web management files. After these files are uploaded, the upload algorithm creates the tar file format.

Caution For the download and upload algorithms to operate properly, do *not* rename image names.

Copying Image Files By Using RCP

You can download a switch module image from an RCP server or upload the image from the switch module to an RCP server.

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

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

Note Instead of using the **copy** privileged EXEC command or the **archive tar** privileged EXEC command, we recommend using the **archive download-sw** and **archive upload-sw** privileged EXEC commands to download and upload software image files.

These sections contain this configuration information:

- Preparing to Download or Upload an Image File By Using RCP, page B-34
- Downloading an Image File By Using RCP, page B-35
- Uploading an Image File By Using RCP, page B-37

Preparing to Download or Upload an Image File By Using RCP

RCP provides another method of downloading and uploading image files between remote hosts and the switch module. Unlike TFTP, which uses User Datagram Protocol (UDP), a connectionless protocol, RCP uses TCP, which is connection-oriented.

To use RCP to copy files, the server from or to which you will be copying files must support RCP. The RCP copy commands rely on the rsh server (or daemon) on the remote system. To copy files by using RCP, you do not need to create a server for file distribution as you do with TFTP. You only need to have access to a server that supports the remote shell (rsh). (Most UNIX systems support rsh.) Because you are copying a file from one place to another, you must have read permission on the source file and write permission on the destination file. If the destination file does not exist, RCP creates it for you.

RCP requires a client to send a remote username on each RCP request to a server. When you copy an image from the switch module to a server by using RCP, the Cisco IOS software sends the first valid username in this list:

- Username specified in the **archive download-sw** or **archive upload-sw** privileged EXEC command if a username is specified
- Username set by the **ip rcmd remote-username** *username* global configuration command if the command is entered
- Remote username associated with the current TTY (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the **username** command, the switch module software sends the Telnet username as the remote username.
- Switch module hostname

For the RCP copy request to execute successfully, an account must be defined on the network server for the remote username. If the server has a directory structure, the image file is written to or copied from the directory associated with the remote username on the server. For example, if the image file resides in the home directory of a user on the server, specify that user's name as the remote username.

Before you begin downloading or uploading an image file by using RCP, do these tasks:

- Ensure that the workstation acting as the RCP server supports the remote shell (rsh).
- Ensure that the switch module has a route to the RCP server. The switch module and the server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the RCP server by using the **ping** command.
- If you are accessing the switch module through the host router's console or a Telnet session and you do not have a valid username, make sure that the current RCP username is the one that you want to use for the RCP download. To view the valid username, you can enter the **show users** privileged EXEC command. If you do not want to use this username, create a new RCP username by using the **ip rcmd remote-username** *username* global configuration command to be used during all archive operations. The new username is stored in NVRAM. If you are accessing the switch module through a Telnet session and you have a valid username, this username is used, and there is no need to set the RCP username. Include the username in the **archive download-sw** or **archive upload-sw** privileged EXEC command if you want to specify a username only for that operation.
- When you upload an image to the RCP to the server, it must be properly configured to accept the RCP write request from the user on the switch module. For UNIX systems, you must add an entry to the .rhosts file for the remote user on the RCP server. For example, suppose the switch module contains these configuration lines:

  ```
  hostname Switch1
  ip rcmd remote-username User0
  ```

  If the switch module IP address translates to *Switch1.company.com*, the .rhosts file for User0 on the RCP server should contain this line:

  ```
  Switch1.company.com Switch1
  ```

For more information, see the documentation for your RCP server.

Downloading an Image File By Using RCP

You can download a new image file and replace or keep the current image.

Beginning in privileged EXEC mode, follow Steps 1 through 6 to download a new image from an RCP server and overwrite the existing image. To keep the current image, go to Step 7.

	Step	Command
Step 1	Verify that the RCP server is properly configured by referring to the "Preparing to Download or Upload an Image File By Using RCP" section on page B-34.	
Step 2	Log into the switch module through the host router's console port or a Telnet session.	
Step 3	Enter global configuration mode. This step is required only if you override the default remote username (see Steps 4 and 5).	**configure terminal**
Step 4	(Optional) Specify the remote username.	**ip rcmd remote-username** *username*
Step 5	Return to privileged EXEC mode.	**end**

	Step	Command
Step 6	Download the image file from the RCP server to the switch module, and overwrite the current image. • The **/overwrite** option overwrites the software image in flash memory with the downloaded image. • For ***//username,*** specify the username. For the RCP copy request to execute successfully, an account must be defined on the network server for the remote username. For more information, see the "Preparing to Download or Upload an Image File By Using RCP" section on page B-34. • For *@location*, specify the IP address of the RCP server. • For ***/directory/image-name*.tar**, specify the directory and the image to download. Directory and image names are case sensitive.	**archive download-sw /overwrite rcp://*username@location/directory/image-name*.tar**
Step 7	Download the image file from the RCP server to the switch module, and keep the current image. • The **/leave-old-sw** option keeps the old software version after a download. • For ***//username,*** specify the username. For the RCP copy request to execute, an account must be defined on the network server for the remote username. For more information, see the "Preparing to Download or Upload an Image File By Using RCP" section on page B-34. • For *@location*, specify the IP address of the RCP server. • **For** ***/directory/image-name*.tar**, specify the directory and the image to download. Directory and image names are case sensitive.	**archive download-sw /leave-old-sw rcp://*username@location/directory/image-name*.tar**
Step 8	After the download and untarring are completed, power cycle the CGR2010.	

The **archive download-sw** command untars/unzips the file. The system prompts you when it completes successfully. The download algorithm verifies that the image is appropriate for the switch module model and that enough DRAM is present, or it aborts the process and reports an error. If you specify the **/overwrite** option, the download algorithm removes the existing image on the flash device whether or not it is the same as the new one and downloads the new image.

If you specify the command without the **/overwrite** option, the download algorithm verifies that the new image is not the same as the one on the switch Flash device. If the images are the same, the download does not occur. If the images are different, the old image is deleted, and the new one is downloaded. If there is not enough space to install the new image and keep the current running image, the download process stops, and an error message is displayed.

Note If the flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the **/overwrite** option.

If you specify the **/leave-old-sw**, the existing files are not removed. If there is not enough room to install the new image an keep the running image, the download process stops, and an error message is displayed.

The algorithm installs the downloaded image onto the system board flash device (flash:). The image is placed into a new directory named with the software version string, and the BOOT environment variable is updated to point to the newly installed image.

If you kept the old software during the download process (you specified the **/leave-old-sw** keyword), you can remove it by entering the **delete /force /recursive** *filesystem***:/***file-url* privileged EXEC command. For *filesystem*, use **flash:** for the system board flash device. For *file-url*, enter the directory name of the old software image. All the files in the directory and the directory are removed.

Caution For the download and upload algorithms to operate properly, do *not* rename image names.

Uploading an Image File By Using RCP

You can upload an image from the switch module to an RCP server. You can later download this image to the same switch module or to another switch module of the same type.

The upload feature should be used only if the web management pages associated with the embedded device manager have been installed with the existing image.

Beginning in privileged EXEC mode, follow these steps to upload an image to an RCP server:

	Step	Command
Step 1	Verify that the RCP server is properly configured by referring to the "Preparing to Download or Upload an Image File By Using RCP" section on page B-34.	
Step 2	Log into the switch module through the host router's console port or a Telnet session.	
Step 3	Enter global configuration mode. This step is required only if you override the default remote username (see Steps 4 and 5).	**configure terminal**
Step 4	(Optional) Specify the remote username.	**ip rcmd remote-username** *username*

	Step	Command
Step 5	Return to privileged EXEC mode.	**end**
Step 6	Upload the currently running switch module image to the RCP server. • For **//***username,* specify the username; for the RCP copy request to execute, an account must be defined on the network server for the remote username. For more information, see the "Preparing to Download or Upload an Image File By Using RCP" section on page B-34. • For **@***location*, specify the IP address of the RCP server. • For **/***directory***/***image-name***.tar**, specify the directory and the name of the software image to be uploaded. Directory and image names are case sensitive. • The *image-name***.tar** is the name of software image to be stored on the server.	**archive upload-sw rcp://***username***@***location***/***directory***/***image-name***.tar**

The **archive upload-sw** privileged EXEC command builds an image file on the server by uploading these files in order: info, the Cisco IOS image, and the web management files. After these files are uploaded, the upload algorithm creates the tar file format.

Caution For the download and upload algorithms to operate properly, do *not* rename image names.

MODBUS TCP Registers

This appendix lists the CGR 2010 ESM-specific read-only registers. MODBUS clients use them to communicate with a MODBUS server (i.e., the switch module). There are no writable registers. For configuration information about MODBUS TCP, see Chapter 16, "MODBUS TCP Configuration."

System Information Registers

Memory address spaces 0x0800 through 0x0FFF are system information registers. Clients use the 0x03 Read Multiple Registers MODBUS function code. The system-information register mapping is as follows:

Table C-1 System Information Registers

Address	# of Registers	Description	R/W	Format	Example/Note for SKU 1	Example/Note for SKU 2
0x0800	64	Product ID	R	Text	"IE9"	"IEA"
0x0840	64	Software image name	R	Text	"grwicdes-ipservicesk9-m"	"grwicdes-ipservicesk9-m"
0x0880	64	Software image version	R	Text	"12.2(58)EY"	"12.2(58)EY"
0x08C0	64	Host name	R	Text	"Switch"	"Switch"
0x0900	1	Number of 10/100 Ethernet ports	R	Uint16	0x4	0x8
0x0901	1	Number of Gigabit Ethernet ports	R	Uint16	0x2	0x2
0x0902	1	CPU board temperature (in Celsius)	R	Uint16	Reads temperature on the switch module CPU board.	Reads temperature on the switch module CPU board.
0x0903	1	Ethernet Switch Module board temperature (in Celsius)	R	Uint16	Reads temperature on the switch module SFP board.	Reads temperature on the switch module SFP board.

Port Information Registers

The port information registers are documented as follows:

- Table C-2 below provides the port information register mapping for the CGR 2010 ESM SFP model (GRWIC-D-ES-6S)
- Table C-3 on page C-4 provides the port information register mapping for the switch's Copper model (GRWIC-D-ES-2S-8PC)
- Table C-4 on page C-7 describes how to interpret the port state values for the switch's SFP model
- Table C-5 on page C-8 describes how to interpret the port state values for the switch's Copper model
- Table C-6 on page C-8 describes the interface-to-LPN mapping for the switch's SFP model
- Table C-7 on page C-8 describes the interface-to-LPN mapping for the switch's Copper model

Port Information Register Mapping for SFP Model (GRWIC-D-ES-6S)

This section provides the port information register mapping for the CGR 2010 ESM SFP model (GRWIC-D-ES-6S).

Memory address spaces 0x1000 through 0x2FFF are interface registers. Clients use the 0x03 Read Multiple Registers MODBUS function code to access the registers.

Table C-2 Port Information Registers, SFP Model

Address in Hex	# of Registers	Description	R/W	Format
1000	64	Port 1 name	R	Text
1040	64	Port 2 name	R	Text
1080	64	Port 3 name	R	Text
10C0	64	Port 4 name	R	Text
1100	64	Port 5 name	R	Text
1140	64	Port 6 name	R	Text
1180	1	Port 1 state	R	Uint16
1181	1	Port 2 state	R	Uint16
1182	1	Port 3 state	R	Uint16
1183	1	Port 4 state	R	Uint16
1184	1	Port 5 state	R	Uint16
1185	1	Port 6 state	R	Uint16
Values for 64-Bit Counters				
1186	4	Port 1 Statistics – Number of packets received	R	Uint64
118A	4	Port 2 Statistics – Number of packets received	R	Uint64
118E	4	Port 3 Statistics – Number of packets received	R	Uint64
1192	4	Port 4 Statistics – Number of packets received	R	Uint64
1196	4	Port 5 Statistics – Number of packets received	R	Uint64
119A	4	Port 6 Statistics – Number of packets received	R	Uint64
119E	4	Port 1 Statistics – Number of packets sent	R	Uint64
11A2	4	Port 2 Statistics – Number of packets sent	R	Uint64

Table C-2 Port Information Registers, SFP Model (continued)

Address in Hex	# of Registers	Description	R/W	Format
11A6	4	Port 3 Statistics – Number of packets sent	R	Uint64
11AA	4	Port 4 Statistics – Number of packets sent	R	Uint64
11AE	4	Port 5 Statistics – Number of packets sent	R	Uint64
11B2	4	Port 6 Statistics – Number of packets sent	R	Uint64
11B6	4	Port 1 Statistics – Number of bytes received	R	Uint64
11BA	4	Port 2 Statistics – Number of bytes received	R	Uint64
11BE	4	Port 3 Statistics – Number of bytes received	R	Uint64
11C2	4	Port 4 Statistics – Number of bytes received	R	Uint64
11C6	4	Port 5 Statistics – Number of bytes received	R	Uint64
11CA	4	Port 6 Statistics – Number of bytes received	R	Uint64
11CE	4	Port 1 Statistics – Number of bytes sent	R	Uint64
11D2	4	Port 2 Statistics – Number of bytes sent	R	Uint64
11D6	4	Port 3 Statistics – Number of bytes sent	R	Uint64
11DA	4	Port 4 Statistics – Number of bytes sent	R	Uint64
11DE	4	Port 5 Statistics – Number of bytes sent	R	Uint64
11E2	4	Port 6 Statistics – Number of bytes sent	R	Uint64
Values for 32-Bit Counters				
11E6	2	Port 1 Statistics – Number of packets received	R	Uint32
11E8	2	Port 2 Statistics – Number of packets received	R	Uint32
11EA	2	Port 3 Statistics – Number of packets received	R	Uint32
11EC	2	Port 4 Statistics – Number of packets received	R	Uint32
11EE	2	Port 5 Statistics – Number of packets received	R	Uint32
11F0	2	Port 6 Statistics – Number of packets received	R	Uint32
11F2	2	Port 1 Statistics – Number of packets sent	R	Uint32
11F4	2	Port 2 Statistics – Number of packets sent	R	Uint32
11F6	2	Port 3 Statistics – Number of packets sent	R	Uint32
11F8	2	Port 4 Statistics – Number of packets sent	R	Uint32
11FA	2	Port 5 Statistics – Number of packets sent	R	Uint32
11FC	2	Port 6 Statistics – Number of packets sent	R	Uint32
11FE	2	Port 1 Statistics – Number of bytes received	R	Uint32
1200	2	Port 2 Statistics – Number of bytes received	R	Uint32
1202	2	Port 3 Statistics – Number of bytes received	R	Uint32
1204	2	Port 4 Statistics – Number of bytes received	R	Uint32
1206	2	Port 5 Statistics – Number of bytes received	R	Uint32
1208	2	Port 6 Statistics – Number of bytes received	R	Uint32

Table C-2 Port Information Registers, SFP Model (continued)

Address in Hex	# of Registers	Description	R/W	Format
120A	2	Port 1 Statistics – Number of bytes sent	R	Uint32
120C	2	Port 2 Statistics – Number of bytes sent	R	Uint32
120E	2	Port 3 Statistics – Number of bytes sent	R	Uint32
1210	2	Port 4 Statistics – Number of bytes sent	R	Uint32
1212	2	Port 5 Statistics – Number of bytes sent	R	Uint32
1214	2	Port 6 Statistics – Number of bytes sent	R	Uint32

Port Information Register Mapping for Copper Model (GRWIC-D-ES-2S-8PC)

This section provides the port information register mapping for the CGR 2010 ESM Copper model (GRWIC-D-ES-2S-8PC).

Memory address spaces 0x1000 through 0x2FFF are interface registers. Clients use the 0x03 Read Multiple Registers MODBUS function code to access the registers.

Table C-3 Port Information Registers, Copper Model

Address in Hex	# of Registers	Description	R/W	Format
1000	64	Port 1 name	R	Text
1040	64	Port 2 name	R	Text
1080	64	Port 3 name	R	Text
10C0	64	Port 4 name	R	Text
1100	64	Port 5 name	R	Text
1140	64	Port 6 name	R	Text
1180	64	Port 7 name	R	Text
11C0	64	Port 8 name	R	Text
1200	64	Port 9 name	R	Text
1240	64	Port 10 name	R	Text
1280	1	Port 1 state	R	Uint16
1281	1	Port 2 state	R	Uint16
1282	1	Port 3 state	R	Uint16
1283	1	Port 4 state	R	Uint16
1284	1	Port 5 state	R	Uint16
1285	1	Port 6 state	R	Uint16
1286	1	Port 7 state	R	Uint16
1287	1	Port 8 state	R	Uint16
1288	1	Port 9 state	R	Uint16

Table C-3 Port Information Registers, Copper Model (continued)

Address in Hex	# of Registers	Description	R/W	Format
1289	1	Port 10 state	R	Uint16
Values for 64-Bit Counters				
128A	4	Port 1 Statistics – Number of packets received	R	Uint64
128E	4	Port 2 Statistics – Number of packets received	R	Uint64
1292	4	Port 3 Statistics – Number of packets received	R	Uint64
1296	4	Port 4 Statistics – Number of packets received	R	Uint64
129A	4	Port 5 Statistics – Number of packets received	R	Uint64
129E	4	Port 6 Statistics – Number of packets received	R	Uint64
12A2	4	Port 7 Statistics – Number of packets received	R	Uint64
12A6	4	Port 8 Statistics – Number of packets received	R	Uint64
12AA	4	Port 9 Statistics – Number of packets received	R	Uint64
12AE	4	Port 10 Statistics – Number of packets received	R	Uint64
12B2	4	Port 1 Statistics – Number of packets sent	R	Uint64
12B6	4	Port 2 Statistics – Number of packets sent	R	Uint64
12BA	4	Port 3 Statistics – Number of packets sent	R	Uint64
12BE	4	Port 4 Statistics – Number of packets sent	R	Uint64
12C2	4	Port 5 Statistics – Number of packets sent	R	Uint64
12C6	4	Port 6 Statistics – Number of packets sent	R	Uint64
12CA	4	Port 7 Statistics – Number of packets sent	R	Uint64
12CE	4	Port 8 Statistics – Number of packets sent	R	Uint64
12D2	4	Port 9 Statistics – Number of packets sent	R	Uint64
12D6	4	Port 10 Statistics – Number of packets sent	R	Uint64
12DA	4	Port 1 Statistics – Number of bytes received	R	Uint64
12DE	4	Port 2 Statistics – Number of bytes received	R	Uint64
12E2	4	Port 3 Statistics – Number of bytes received	R	Uint64
12E6	4	Port 4 Statistics – Number of bytes received	R	Uint64
12EA	4	Port 5 Statistics – Number of bytes received	R	Uint64
12EE	4	Port 6 Statistics – Number of bytes received	R	Uint64
12F2	4	Port 7 Statistics – Number of bytes received	R	Uint64
12F6	4	Port 8 Statistics – Number of bytes received	R	Uint64
12FA	4	Port 9 Statistics – Number of bytes received	R	Uint64

Table C-3 Port Information Registers, Copper Model (continued)

Address in Hex	# of Registers	Description	R/W	Format
12FE	4	Port 10 Statistics – Number of bytes received	R	Uint64
1302	4	Port 1 Statistics – Number of bytes sent	R	Uint64
1306	4	Port 2 Statistics – Number of bytes sent	R	Uint64
130A	4	Port 3 Statistics – Number of bytes sent	R	Uint64
130E	4	Port 4 Statistics – Number of bytes sent	R	Uint64
1312	4	Port 5 Statistics – Number of bytes sent	R	Uint64
1316	4	Port 6 Statistics – Number of bytes sent	R	Uint64
131A	4	Port 7 Statistics – Number of bytes sent	R	Uint64
131E	4	Port 8 Statistics – Number of bytes sent	R	Uint64
1322	4	Port 9 Statistics – Number of bytes sent	R	Uint64
1326	4	Port 10 Statistics – Number of bytes sent	R	Uint64
Values for 32-Bit Counters				
132A	2	Port 1 Statistics – Number of packets received	R	Uint32
132C	2	Port 2 Statistics – Number of packets received	R	Uint32
132E	2	Port 3 Statistics – Number of packets received	R	Uint32
1330	2	Port 4 Statistics – Number of packets received	R	Uint32
1332	2	Port 5 Statistics – Number of packets received	R	Uint32
1334	2	Port 6 Statistics – Number of packets received	R	Uint32
1336	2	Port 7 Statistics – Number of packets received	R	Uint32
1338	2	Port 8 Statistics – Number of packets received	R	Uint32
133A	2	Port 9 Statistics – Number of packets received	R	Uint32
133C	2	Port 10 Statistics – Number of packets received	R	Uint32
133E	2	Port 1 Statistics – Number of packets sent	R	Uint32
1340	2	Port 2 Statistics – Number of packets sent	R	Uint32
1342	2	Port 3 Statistics – Number of packets sent	R	Uint32
1344	2	Port 4 Statistics – Number of packets sent	R	Uint32
1346	2	Port 5 Statistics – Number of packets sent	R	Uint32
1348	2	Port 6 Statistics – Number of packets sent	R	Uint32
134A	2	Port 7 Statistics – Number of packets sent	R	Uint32
134C	2	Port 8 Statistics – Number of packets sent	R	Uint32
134E	2	Port 9 Statistics – Number of packets sent	R	Uint32
1350	2	Port 10 Statistics – Number of packets sent	R	Uint32
1352	2	Port 1 Statistics – Number of bytes received	R	Uint32
1354	2	Port 2 Statistics – Number of bytes received	R	Uint32
1356	2	Port 3 Statistics – Number of bytes received	R	Uint32

Table C-3 Port Information Registers, Copper Model (continued)

Address in Hex	# of Registers	Description	R/W	Format
1358	2	Port 4 Statistics – Number of bytes received	R	Uint32
135A	2	Port 5 Statistics – Number of bytes received	R	Uint32
135C	2	Port 6 Statistics – Number of bytes received	R	Uint32
135E	2	Port 7 Statistics – Number of bytes received	R	Uint32
1360	2	Port 8 Statistics – Number of bytes received	R	Uint32
1362	2	Port 9 Statistics – Number of bytes received	R	Uint32
1364	2	Port 01 Statistics – Number of bytes received	R	Uint32
1366	2	Port 1 Statistics – Number of bytes sent	R	Uint32
1368	2	Port 2 Statistics – Number of bytes sent	R	Uint32
136A	2	Port 3 Statistics – Number of bytes sent	R	Uint32
136C	2	Port 4 Statistics – Number of bytes sent	R	Uint32
136E	2	Port 5 Statistics – Number of bytes sent	R	Uint32
1370	2	Port 6 Statistics – Number of bytes sent	R	Uint32
1372	2	Port 7 Statistics – Number of bytes sent	R	Uint32
1374	2	Port 8 Statistics – Number of bytes sent	R	Uint32
1376	2	Port 9 Statistics – Number of bytes sent	R	Uint32
1378	2	Port 10 Statistics – Number of bytes sent	R	Uint32

Interpreting the Port State for the Switch Module SFP Model

Table C-4 Port Information: Interpreting the Port State for GRWIC-D-6S (SFP Model)

Address	Description	Value
0x1180 to 0x1185	Port 1 state to Port 6 state	The upper byte represents the interface state: • 0x0: Interface is down • 0x1: Interface is going down • 0x2: Interface is in the initializing state • 0x3: Interface is coming up • 0x4: Interface is up and running • 0x5: Interface is reset by the user • 0x6: Interface is shut down by the user • 0x7: Interface is being deleted The lower byte represents the line protocol state: • 0x1: Line protocol state is up • 0x0: Line protocol state is down

Interpreting the Port State for the Switch Module Copper Model

Table C-5 Port Information: Interpreting the Port State for GRWIC-D-2S-8PC (Copper Model)

Address	Description	Value
0x1280 to 0x1289	Port 1 state to Port 6 state	The upper byte represents the interface state: • 0x0: Interface is down • 0x1: Interface is going down • 0x2: Interface is in the initializing state • 0x3: Interface is coming up • 0x4: Interface is up and running • 0x5: Interface is reset by the user • 0x6: Interface is shut down by the user • 0x7: Interface is being deleted The lower byte represents the line protocol state: • 0x1: Line protocol state is up • 0x0: Line protocol state is down

Interface-to-LPN Mapping for the Switch Module SFP Model

Table C-6 Interface-to-LPN Mapping for GRWIC-D-6S (SFP Model)

Interface	LPN
Fast Ethernet 0/1	1
Fast Ethernet 0/2	2
Fast Ethernet 0/3	3
Fast Ethernet 0/4	4
Gigabit Ethernet 0/1	13
Gigabit Ethernet 0/2	14

Interface-to-LPN Mapping for the Switch Module Copper Model

Table C-7 Interface-to-LPN Mapping for GRWIC-D-2S-8PC (Copper Model)

Interface	LPN
Fast Ethernet 0/1	1
Fast Ethernet 0/2	2
Fast Ethernet 0/3	3
Fast Ethernet 0/4	4

Table C-7 Interface-to-LPN Mapping for GRWIC-D-2S-8PC (Copper Model)

Interface	LPN
Fast Ethernet 0/5	5
Fast Ethernet 0/6	6
Fast Ethernet 0/7	7
Fast Ethernet 0/8	8
Gigabit Ethernet 0/1	17
Gigabit Ethernet 0/2	18

Unsupported Commands in Cisco IOS Release 12.2(58)EZ

This appendix lists some of the command-line interface (CLI) commands that appear when you enter the question mark (?) at the CGR 2010 ESM switch prompt but are not supported in this release, either because they are not tested or because of switch hardware limitations. This is not a complete list. The unsupported commands are listed by software feature and command mode.

This appendix contains the following topics:

Access Control List Commands

Unsupported Global Configuration Commands

access-list rate-limit *acl-index* {*precedence* | **mask** *prec-mask*}

access-list dynamic extended

Unsupported Privileged EXEC Commands

access-enable [**host**] [**timeout** *minutes*]

access-template [*access-list-number* | *name*] [*dynamic-name*] [*source*] [*destination*] [**timeout** *minutes*]

clear access-template [*access-list-number* | *name*] [*dynamic-name*] [*source*] [*destination*].

ARP Commands

Unsupported Global Configuration Commands

arp *ip-address hardware-address* **smds**

arp *ip-address hardware-address* **srp-a**

arp *ip-address hardware-address* **srp-b**

Unsupported Interface Configuration Commands

arp probe

ip probe proxy

Boot Loader Commands

Unsupported Global Configuration Command

boot buffersize

Unsupported User EXEC Command

verify

Debug Commands

debug dot1x feature

debug platform cli-redirection main

debug platform configuration

debug qos

Embedded Event Manager Commands

Unsupported Applet Configuration Commands

no event interface name [*interface-name*] **parameter** [*counter-name*] entry-val [*entry counter value*] **entry-op** {*gt* | *ge* | *eq* | *ne* |*lt* | *le*} [**entry-type {increment | rate | value**] [**exit-va**l [*exit value*] **exit-op** {*gt* | *ge* | *eq* | *ne* |*lt* | *le*} **exit-type { increment | rate | value}**][**average-factor <average-factor-value>**]

no trigger

tag

Unsupported Global Configuration Commands

no event manager directory user repository [*url location*]

event manager applet [*applet-name*] maxrun

Unsupported Privileged EXEC Commands

event manager update user policy [*policy-filename* | *group* [*group name expression*]] | *repository* [*url location*]

Parameters are not supported for this command:

event manager run [*policy name*] |***<paramater1>***|... ***<paramater15>***|

HSRP Commands

Unsupported Global Configuration Commands

interface Async

interface BVI

interface Dialer

interface Group-Async

interface Lex

interface Multilink

interface Virtual-Template

interface Virtual-Tokenring

Unsupported Interface Configuration Commands

mtu

standby mac-refresh *seconds*

standby use-bia

IEEE 802.1x Commands

Unsupported Interface Configuration Commands

dot1x credentials

Note The **dot1x credentials** *profile* global configuration command is still supported.

dot1x max-start

Unsupported Privileged EXEC Commands

clear eap sessions

dot1x re-authenticate

show eap

IGMP Snooping Commands

Unsupported Global Configuration Commands

ip igmp snooping source-only-learning

Interface Commands

Unsupported Global Configuration Commands

interface tunnel

Unsupported Interface Configuration Commands

power inline port priority *high* | *low*

transmit-interface *type number*

Unsupported Privileged EXEC Commands

show interfaces [*interface-id* | **vlan** *vlan-id*] [**crb** | **fair-queue** | **irb** | **mac-accounting** | **precedence** | **irb** | **random-detect** | **rate-limit** | **shape**]

IP Multicast Routing Commands

Unsupported Global Configuration Commands

All **ip dvmrp** commands

ip multicast-routing vrf *vrf-name*

ip pim accept-rp {*address* | **auto-rp**} [*group-access-list-number*]

ip pim message-interval *seconds*

ip pim register-rate-limit

Unsupported Interface Configuration Commands

frame-relay ip rtp header-compression [**active** | **passive**]

frame-relay map ip *ip-address dlci* [**broadcast**] **compress**

frame-relay map ip *ip-address dlci* **rtp header-compression** [**active** | **passive**]

All **ip dvmrp** commands

ip igmp helper-address *ip-address*

ip multicast helper-map {*group-address* | **broadcast**} {*broadcast-address* | *multicast-address*} *extended-access-list-number*

ip multicast rate-limit {**in** | **out**} [**video** | **whiteboard**] [**group-list** *access-list*] [**source-list** *access-list*] *kbps*

ip multicast ttl-threshold *ttl-value* (instead, use the **ip multicast boundary** *access-list-number* interface configuration command)

ip multicast use-functional

ip pim minimum-vc-rate *pps*

ip pim multipoint-signalling

ip pim nbma-mode

ip pim vc-count *number*

ip rtp compression-connections *number*

ip rtp header-compression [**passive**]

Unsupported Privileged EXEC Commands

clear ip rtp header-compression [*type number*]

clear ip dvmrp route commands

debug ip dvmrp commands

The **debug ip packet** command displays packets received by the switch CPU. It does not display packets that are hardware-switched.

The **debug ip mcache** command affects packets received by the switch CPU. It does not display packets that are hardware-switched.

The **debug ip mpacket** [**detail**] [*access-list-number* [*group-name-or-address*] command affects only packets received by the switch CPU. Because most multicast packets are hardware-switched, use this command only when you know that the route will forward the packet to the CPU.

debug ip pim atm

show frame-relay ip rtp header-compression [**interface** *type number*]

show ip dvmrp route commands

The **show ip mcache** command displays entries in the cache for those packets that are sent to the switch CPU. Because most multicast packets are switched in hardware without CPU involvement, you can use this command, but multicast packet information is not displayed.

The **show ip mpacket** commands are supported but are only useful for packets received at the switch CPU. If the route is hardware-switched, the command has no effect because the CPU does not receive the packet and cannot display it.

show ip pim vc [*group-address* | *name*] [*type number*]

show ip rtp header-compression [*type number*] [**detail**]

IP Unicast Routing Commands

Unsupported BGP Router Configuration Commands

address-family vpnv4

default-information originate

neighbor advertise-map

neighbor allowas-in

neighbor default-originate

neighbor description

network backdoor

table-map

Unsupported Global Configuration Commands

ip accounting-list *ip-address wildcard*

ip as-path access-list

ip accounting-transits *count*

ip cef accounting [**per-prefix**] [**non-recursive**]

ip cef traffic-statistics [**load-interval** *seconds*] [**update-rate** *seconds*]]

ip flow-aggregation

ip flow-cache

ip flow-export

ip gratuitous-arps

ip local

ip prefix-list

ip reflexive-list

router egp

router-isis

router iso-igrp

router mobile

router odr

router static

Unsupported Interface Configuration Commands

dampening

ip load-sharing [**per-packet**]

ip accounting

ip load-sharing [**per-packet**]

ip mtu *bytes*

ip ospf dead-interval minimal hello-multiplier *multiplier*

ip verify

ip unnumbered *type number*

All **ip security** commands

Unsupported Privileged EXEC or User EXEC Commands

clear ip accounting [**checkpoint**]

clear ip bgp *address* flap-statistics

clear ip bgp prefix-list

debug ip cef stats

show cef [**drop** | **not-cef-switched**]

show ip accounting [**checkpoint**] [**output-packets** | **access-violations**]

show ip bgp dampened-paths

show ip bgp inconsistent-as

show ip bgp regexp *regular expression*

show ip prefix-list *regular expression*

show ipv6 (all)

Unsupported Route Map Commands

match route-type for policy-based routing (PBR)

set as-path {**tag** | **prepend** *as-path-string*}

set automatic-tag

set dampening *half-life reuse suppress max-suppress-time*

set default interface *interface-id* [*interface-id.....*]

set interface *interface-id* [*interface-id.....*]

set ip default next-hop *ip-address* [*ip-address.....*]

set ip destination *ip-address mask*

set ip precedence *value*

set ip *qos-group*

set metric-type internal

set origin

set metric-type internal

set tag *tag-value*

Unsupported VPN Configuration Commands

All

MAC Address Commands

Unsupported Global Configuration Commands

mac-address-table aging-time

mac-address-table notification

mac-address-table static

Unsupported Privileged EXEC Commands

show mac-address-table

show mac-address-table address

show mac-address-table aging-time

show mac-address-table count

show mac-address-table dynamic

show mac-address-table interface

show mac-address-table multicaset

show mac-address-table notification

show mac-address-table static

show mac-address-table vlan

show mac address-table multicast

Note Use the **show ip igmp snooping groups** privileged EXEC command to display Layer 2 multicast address-table entries for a VLAN.

Miscellaneous Commands

Unsupported Global Configuration Commands

exception crashinfo

errdisable detect cause dhcp-rate-limit

errdisable recovery cause dhcp-rate-limit

errdisable recovery cause unicast flood

l2protocol-tunnel global drop-threshold

memory reserve critical

power inline consumption default *wattage*

service compress-config

Unsupported Privileged EXEC Commands

archive config

file verify auto

remote command all

show archive config

show archive log

show cable-diagnostics prbs

show power inline

test cable-diagnostics prbs

stack-mac persistent timer

track *object-number* **rtr**

Unsupported *show platform* Commands

show platform ip unicast vrf {**compaction** | **tcam-label**}

show platform ipv6 unicast

show platform tb

Unsupported User EXEC Commands

verify

MSDP Commands

Unsupported Global Configuration Commands

ip msdp default-peer *ip-address* | *name* [**prefix-list** *list*] (Because BGP/MBGP is not supported, use the **ip msdp peer** command instead of this command.)

Unsupported Privileged EXEC Commands

show access-expression

show exception

show location

show pm LINE

show smf [*interface-id*]

show subscriber-policy [*policy-number*]

show template [*template-name*]

NetFlow Commands

Unsupported Global Configuration Commands

ip flow-aggregation cache

ip flow-cache entries

ip flow-export

QoS Commands

Unsupported Global Configuration Command

priority-list

Unsupported Interface Configuration Command

priority-group

Unsupported policy-map Class Police Configuration Mode Command

conform-color *class-map* **police configuration**

RADIUS Commands

Unsupported Global Configuration Commands

aaa authentication *feature* **default enable**

aaa authentication *feature* **default line**

aaa nas port extended

authentication command bounce-port ignore

authentication command disable-port ignore

radius-server attribute nas-port

radius-server configure

radius-server extended-portnames

SNMP Commands

Unsupported Global Configuration Commands

snmp-server enable informs

snmp-server ifindex persist

Spanning Tree Commands

Unsupported Global Configuration Command

spanning-tree pathcost method {long | short}

spanning-tree transmit hold-count

Unsupported Interface Configuration Command

spanning-tree stack-port

VLAN Commands

Unsupported Global Configuration Command

vlan internal allocation policy {ascending | descending}

Unsupported User EXEC Commands

show running-config vlan

show vlan ifindex

vlan database

Unsupported VLAN Database Commands

vtp

vlan