ES3528M
ES3552M
Fast Ethernet Switch

Management Guide

www.edge-core.com

MANAGEMENT GUIDE

FAST ETHERNET SWITCH

Layer 2 Switch
with 24/48 10/100BASE-TX (RJ-45) Ports,
and 4 Gigabit Combination Ports (RJ-45/SFP)

ES3528M
ES3552M
E082010/ST-R05
149100010700H

About This Guide

Purpose This guide gives specific information on how to operate and use the management functions of the switch.

Audience The guide is intended for use by network administrators who are responsible for operating and maintaining network equipment; consequently, it assumes a basic working knowledge of general switch functions, the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

Conventions The following conventions are used throughout this guide to show information:

Note: Emphasizes important information or calls your attention to related features or instructions.

Caution: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Warning: Alerts you to a potential hazard that could cause personal injury.

Related Publications The following publication details the hardware features of the switch, including the physical and performance-related characteristics, and how to install the switch:

The *Installation Guide*

Also, as part of the switch's software, there is an online web-based help that describes all management related features.

REVISION HISTORY

This section summarizes the changes in each revision of this guide.

AUGUST 2010 REVISION

This is the fifth version of this guide. This guide is valid for software release v1.4.8.0. It includes information on the following changes to web pages or command line interface:

- Added "Downloading a Configuration File Referenced by a DHCP Server" on page 73.
- Added description of DHCP Relay Option 82, DHCP Relay Option 82 Policy, and DHCP Relay Server parameters on the IP Configuration page (see "Setting the Switch's IP Address" on page 100).
- Added "Displaying CPU Utilization" on page 106.
- Added "Displaying Memory Utilization" on page 107.
- Added User Authentication Traps (see "Specifying Trap Managers and Trap Types" on page 147).
- Added "Configuring MAC Notification Traps for Interfaces" on page 150.
- Added macNotificationTrap to Table 10, "Supported Notification Messages," on page 159.
- Added Supplicant Port Configuration page (see "Configuring Supplicant Port Settings for 802.1X" on page 206).
- Added Supplicant Statistics page (see "Displaying 802.1X Supplicant Statistics" on page 209).
- Updated information in the Command Usage section under "Network Access (MAC Address Authentication)" on page 215.
- Added "Showing TCAM Utilization" on page 237.
- Added "Configuring VLAN Settings for ARP Inspection" on page 241.
- Added "Configuring Interface Settings for ARP Inspection" on page 243.
- Added "Displaying ARP Inspection Statistics" on page 245.
- Added "VLAN Trunking" on page 285.
- Added "Performing Cable Diagnostics" on page 287.
- Added description of Port Utilization parameter in the Port Statistics page (see "Showing Port or Trunk Statistics" on page 288).
- Added "Layer 2 Protocol Tunneling" on page 323.
- Updated information about the maximum string length for VLAN names under "Configuring VLAN Groups" on page 333,

- Updated information about limitations on the number of rules in a class map in the Overview section under "Quality of Service" on page 383, under "Configuring a Class Map" on page 384.
- Updated information about limitations on the number of policy maps in the Command Usage section under "Creating QoS Policies" on page 387.
- Updated the Syntax section and information in the Command Usage section under "show running-config" on page 465.
- Added the command "delete non-active" on page 476.
- Added line "accounting commands" on page page 481.
- Added the command "show upgrade" on page 481.
- Added user-authentication parameter to the snmp-server enable traps command (page 539).
- Added the commands "snmp-server enable traps mac-notification" on page 542, "snmp-server enable port-traps mac-notification" on page 543, and "show snmp-server enable port-traps interface" on page 544.
- Added the command "accounting commands" on page 573.
- Added "PPPoE Intermediate Agent" on page 606.
- Added the command "ip source-guard max-binding" on page 647.
- Added "time-range" parameter to the commands "permit, deny (Standard IP ACL)" on page 662, "permit, deny (Extended IPv4 ACL)" on page 663, "ip access-group" on page 665, "permit, deny (Standard IPv6 ACL)" on page 668, "permit, deny (Extended IPv6 ACL)" on page 669, "ipv6 access-group" on page 671, "permit, deny (MAC ACL)" on page 673, and "mac access-group" on page 675.
- Added the command "mdix" on page 686.
- Added the command "show interfaces transceiver" on page 697.
- Added the commands "test cable-diagnostics tdr interface" on page 698, and "show cable-diagnostics" on page 699.
- Added the command "spanning-tree cisco-prestandard" on page 745
- Updated information in the Command Usage section for the "spanning-tree pathcost method" on page 749.
- Updated information in the Syntax section under "show spanning-tree" on page 768.
- Added "EAPS Commands" on page 771.

- Added "ERPS Commands" on page 785.
- Updated information about the maximum string length for VLAN names under "vlan" on page 805.
- Added the command "switchport dot1q-tunnel service match cvid" on page 817.
- Added the commands "l2protocol-tunnel tunnel-dmac" on page 819, "switchport l2protocol-tunnel" on page 820, and "show l2protocol-tunnel" on page 821.
- Updated information about limitations on the number of rules in a class map under "Quality of Service Commands" on page 853, "class-map" on page 854, and "match" on page 855.
- Updated information about limitations on the number of policy maps in the Command Usage section under "class" on page 858, and under "police" on page 859.
- Added "show ip igmp snooping groups" on page 870.
- Added "MLD Snooping Commands" on page 897.
- Updated information in the Syntax section under "ip dhcp relay information option" on page 938.
- Updated information in the Syntax section under "ip address" on page 944.
- Updated information in "Using System Logs" on page 956.

APRIL 2009 REVISION

This is the fourth revision of this guide. This guide is valid for software release v1.3.4.0. It includes information on the following changes to web pages or command line interface:

- Added information on new features in Table 1-1, "Key Features," on page 1-1 and "Description of Software Features" on page 2.
- Added new menu items to Table 3-2, "Main Menu," on page 3-4, including Auto Operation Code Upgrade, HTTP Upgrade/Download, SNTP Current Time, SNTP Summer Time, sFlow, ARP Inspection, LACP Aggregation Group, Multicast Control, Unknown Unicast Control, STA Edge Port Configuration, VLAN Traffic Segmentation, VLAN Mirror Configuration, IP Subnet VLAN, MAC Based VLAN, MVR Receiver Configuration, MVR Receiver Group IP Information, MVR Receiver Group Member Configuration, and DNS.
- Updated information under "Managing Firmware" on page 22 about file transfer with FTP server, and automatic upgrade of run-time code.
- Updated information under "Saving or Restoring Configuration Settings" on page 28 about file transfer with FTP server.

- Added "Uploading and Downloading Files Using HTTP" on page 30.
- Updated information under "Sending Simple Mail Transfer Protocol Alerts" on page 39
- Added "Configuring Summer Time" on page 47.
- Updated information under "Specifying Trap Managers and Trap Types" on page 52.
- Added "Sampling Traffic Flows" on page 65.
- Added information about using dynamic QoS profiles under "Network Access (MAC Address Authentication)" on page 114.
- Added description of MAC Address Aging under "Configuring the MAC Authentication Rea ut hen tic at ion Time" on page 116.
- Added "MAC Filter Configuration" on page 121.
- Added information under "Access Control Lists" on page 123 about IPv6 ACLs and ARP ACLs.
- Added "ARP Inspection" on page 135.
- Added Command Usage section under "DHCP Snooping VLAN Configuration" on page 144.
- Added Command Usage section under "DHCP Snooping Information Option Configuration" on page 145.
- Added Command Usage section under "Configuring Ports for DHCP Snooping" on page 146.
- Updated information in Command Attributes section under "Displaying DHCP Snooping Binding Information" on page 148.
- Updated information in Command Usage section under "Configuring Ports for IP Source Guard" on page 149.
- Updated infromation in Command Usage section under "Configuring Static Binding for IP Source Guard" on page 151.
- Added information in Field Attributes (CLI) section under "Displaying Connection Status" on page 154.
- Added information in Command Attributes section under "Configuring Interface Connections" on page 156.
- Added information in Command Usage section under "Setting Broadcast Storm Thresholds" on page 171
- Added "Setting Multicast Storm Thresholds" on page 173.

- Added "Setting Unknown Unicast Storm Thresholds" on page 174.
- Added "Configuring Port and Trunk Loopback Detection" on page 189.
- Updated information in Field Attributes section under "Displaying Global Settings for STA" on page 190.
- Updated information in Command Attributes section under "Configuring Global Settings for STA" on page 193.
- Updated information in Field Attributes section under "Displaying Interface Settings for STA" on page 197.
- Updated information in Command Attributes section under "Configuring Interface Settings for STA" on page 200.
- Added "Spanning Tree Edge Port Configuration" on page 203.
- Updated information in Field Attributes section under "Configuring Interface Settings for MSTP" on page 210.
- Updated information in Command Attributes section under "Configuring VLAN Behavior for Interfaces" on page 222.
- Updated information under "Protocol VLANs" on page 238.
- Added Command Usage section under "Mapping Protocols to VLANs" on page 240.
- Added "Configuring VLAN Mirroring" on page 241.
- Added "Configuring IP Subnet VLANs" on page 242.
- Added "Configuring MAC-based VLANs" on page 243.
- Added Field Attributes section under "Displaying LLDP Local Device Information" on page 249.
- Added Field Attributes section under "Displaying LLDP Remote Port Information" on page 252.
- Added Field Attributes section under "Displaying LLDP Remote Information Details" on page 253.
- Added Field Attributes section under "Displaying Device Statistics" on page 255.
- Added Field Attributes section under "Displaying Detailed Device Statistics" on page 256.
- Added Command Usage section and updated information in Command Attributes section under "Selecting the Queue Mode" on page 261.

- Updated information under "Mapping Layer 3/4 Priorities to CoS Values" on page 264.
- Updated information under "Multicast Filtering" on page 279.
- Updated information under "Enabling IGMP Immediate Leave" on page 283.
- Updated information under "Configuring Global MVR Settings" on page 295.
- Updated information in Attributes section under "Displaying MVR Interface Status" on page 297.
- Added "Domain Name Service" on page 305.
- Updated information in Command Usage section under "Switch Clustering" on page 310.
- Updated information under "UPnP" on page 315.
- Added new command groups to "Command Groups" on page 4-10, including Flow Sampling, Automatic Traffic Control, and Domain Name Service.
- Added the command "reload (Global Configuration)" on page 4-14.
- Updated information under "File Management Commands" on page 4-36 about using an FTP server and automatic upgrade of run-time code.
- Updated information under "copy" on page 4-37.
- Added terminal configuration commands under "Line Commands" on page 4-44.
- Updated information under the command "show logging" on page 4-61.
- Added "Using Switch Clustering" section under "Switch Cluster Commands" on page 4-80.
- Added ATC Trap Commands to Table 4-21, "SNMP Commands," on page 4-87.
- Added "Flow Sampling Commands" on page 4-102.
- Added new commands to "User Account and Privilege Level Commands" on page 4-109.
- Added Command Usage section under "dot1x re-authenticate" on page 4-148.
- Added Command Usage section under "dot1x re-authentication" on page 4-149.

- Added new commands under "Network Access (MAC Address Authentication)" on page 4-160.
- Added Command Usage section under "network-access dynamic-qos" on page 4-167.
- Updated information in Command Usage section under "ip dhcp snooping trust" on page 4-181.
- Updated information in Command Usage section under "ip dhcp snooping information option" on page 4-183.
- Updated information under "ip dhcp snooping information policy" on page 4-184.
- Updated information in Command Usage section under "ip source-guard" on page 4-186.
- Added "ARP Inspection Commands" on page 4-190.
- Added the command "access-list rule-mode" on page 4-199.
- Updated information under "permit, deny (Extended IPv4 ACL)" on page 4-202.
- Added "IPv6 ACLs" on page 4-205.
- Added "ARP ACLs" on page 4-210.
- Updated information under "permit, deny (MAC ACL)" on page 4-215.
- Updated information in Command Usage section under "speed-duplex" on page 4-221.
- Added the command "media-type" on page 4-225.
- Added the command "giga-phy-mode" on page 4-225.
- Updated information under "switchport packet-rate" on page 4-227.
- Added "Automatic Traffic Control Commands" on page 4-233.
- Added the commands "lacp active/passive" on page 4-255.
- Updated information under "port monitor" on page 4-260.
- Updated information under "show port monitor" on page 4-261.
- Added new commands to "Spanning Tree Commands" on page 4-268.
- Added the command "spanning-tree system-bpdu-flooding" on page 4-273.
- Updated information under "spanning-tree cost" on page 4-279.

- Updated information under "spanning-tree edge-port" on page 4-281.
- Added the command "spanning-tree bpdu-filter" on page 4-283.
- Added the command "spanning-tree bpdu-guard" on page 4-284.
- Added the command "spanning-tree port-bpdu-flooding" on page 4-284.
- Added the command "spanning-tree root-guard" on page 4-285.
- Added the command "spanning-tree loopback-detection" on page 4-286.
- Added the command "spanning-tree loopback-detection release-mode" on page 4-287.
- Added the command "spanning-tree loopback-detection trap" on page 4-288.
- Updated information under "spanning-tree mst cost" on page 4-288.
- Added new Command Groups in Table 4-70, "VLAN Command Groups," on page 4-293.
- Updated information under "switchport mode" on page 4-301.
- Updated information under "switchport allowed vlan" on page 4-304.
- Added the command "vlan-trunking" on page 4-305.
- Added "Limitations on QinQ" section under "Configuring IEEE 802.1Q Tunneling" on page 4-308.
- Updated information under "switchport dot1q-tunnel mode" on page 4-309.
- Added "Configuring Port-based Traffic Segmentation" on page 4-312.
- Updated information in Command Usage section under "private-vlan" on page 4-317.
- Added "Configuring IP Subnet VLANs" on page 4-324.
- Added "Configuring MAC Based VLANs" on page 4-326.
- Added the command "rename" on page 4-368.
- Added the command "description" on page 4-368.
- Updated information under "mvr (Global Configuration)" on page 4-392
- Updated information under "mvr (Interface Configuration)" on page 4-394

- Updated information under "show mvr" on page 4-396
- Added "Domain Name Service Commands" on page 4-399.
- Added the command "show arp" on page 4-409.

DECEMBER 2007 REVISION

This is the third revision of this guide.

DECEMBER 2006 REVISION

This is the second revision of this guide.

SEPTEMBER 2006 REVISION

This is the first revision of this guide.

CONTENTS

FIGURES

TABLES

SECTION I

GETTING STARTED

This section provides an overview of the switch, and introduces some basic concepts about network switches. It also describes the basic settings required to access the management interface.

This section includes these chapters:

1 INTRODUCTION

This switch provides a broad range of features for Layer 2 switching. It includes a management agent that allows you to configure the features listed in this manual. The default configuration can be used for most of the features provided by this switch. However, there are many options that you should configure to maximize the switch's performance for your particular network environment.

KEY FEATURES

Table 1: Key Features

Feature	Description
Configuration Backup and Restore	Using management station or FTP/TFTP server
Authentication	Console, Telnet, web – user name/password, RADIUS, TACACS+ Port – IEEE 802.1X, MAC address filtering SNMP v1/2c - Community strings SNMP version 3 – MD5 or SHA password Telnet – SSH Web – HTTPS
General Security Measures	AAA ARP inspection DHCP Snooping (with Option 82 relay information) IP Source Guard Network Access – MAC Address Authentication Private VLANs Port Authentication – IEEE 802.1X Port Security – MAC address filtering Web Authentication – Web access with RADIUS Authentication
Access Control Lists	Supports IP and MAC ACLs, 100 rules per system
DHCP	Client
DNS	Client and Proxy service
Port Configuration	Speed and duplex mode and flow control
Port Trunking	Supports up to 8 trunks – static or dynamic trunking (LACP)
Port Mirroring	One or more source ports to one analysis port
Congestion Control	Rate Limiting Throttling for broadcast, multicast, unknown unicast storms
Address Table	8K MAC addresses in the forwarding table, 1K static MAC addresses, 256 L2 multicast groups
IEEE 802.1D Bridge	Supports dynamic data switching and addresses learning
Store-and-Forward Switching	Supported to ensure wire-speed switching while eliminating bad frames

Table 1: Key Features (Continued)

Feature	Description
Spanning Tree Algorithm	Supports standard STP, Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Trees (MSTP)
Virtual LANs	Up to 255 using IEEE 802.1Q, port-based, protocol-based, private VLANs, and voice VLANs
Traffic Prioritization	Default port priority, traffic class map, queue scheduling, or Differentiated Services Code Point (DSCP)
Qualify of Service	Supports Differentiated Services (DiffServ)
Link Layer Discovery Protocol	Used to discover basic information about neighboring devices
Multicast Filtering	Supports IGMP snooping, query, profile filtering, MLD snooping, and Multicast VLAN Registration
Switch Clustering	Supports up to 36 member switches in a cluster
Tunneling	Supports IEEE 802.1Q tunneling (QinQ)

DESCRIPTION OF SOFTWARE FEATURES

The switch provides a wide range of advanced performance enhancing features. Flow control eliminates the loss of packets due to bottlenecks caused by port saturation. Storm suppression prevents broadcast, multicast or unknown unicast traffic storms from engulfing the network. Port-based, protocol based and private VLANs, plus support for automatic GVRP VLAN registration provide traffic security and efficient use of network bandwidth. CoS priority queueing ensures the minimum delay for moving real-time multimedia data across the network. While multicast filtering provides support for real-time network applications. Some of the management features are briefly described below.

CONFIGURATION BACKUP AND RESTORE

You can save the current configuration settings to a file on the management station (using the web interface) or an FTP/TFTP server (using the web or console interface), and later download this file to restore the switch configuration settings.

AUTHENTICATION

This switch authenticates management access via the console port, Telnet, or a web browser. User names and passwords can be configured locally or can be verified via a remote authentication server (i.e., RADIUS or TACACS+). Port-based authentication is also supported via the IEEE 802.1X protocol. This protocol uses Extensible Authentication Protocol over LANs (EAPOL) to request user credentials from the 802.1X client, and then verifies the client's right to access the network via an authentication server.

Other authentication options include HTTPS for secure management access via the web, SSH for secure management access over a Telnet-equivalent connection, SNMP Version 3, IP address filtering for SNMP/Telnet/web management access. MAC address filtering and IP source guard also

provide authenticated port access. While DHCP snooping is provided to prevent malicious attacks from insecure ports

ACCESS CONTROL LISTS ACLs provide packet filtering for IPv4 frames (based on address, protocol, Layer 4 protocol port number or TCP control code), IPv6 frames (based on address, next header type, or flow label), or any frames (based on MAC address or Ethernet type). ACLs can be used to improve performance by blocking unnecessary network traffic or to implement security controls by restricting access to specific network resources or protocols.

PORT CONFIGURATION You can manually configure the speed, duplex mode, and flow control used on specific ports, or use auto-negotiation to detect the connection settings used by the attached device. Use full-duplex mode on ports whenever possible to double the throughput of switch connections. Flow control should also be enabled to control network traffic during periods of congestion and prevent the loss of packets when port buffer thresholds are exceeded. The switch supports flow control based on the IEEE 802.3x standard (now incorporated in IEEE 802.3-2002).

RATE LIMITING This feature controls the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Packets that exceed the acceptable amount of traffic are dropped.

PORT MIRRORING The switch can unobtrusively mirror traffic from any port, VLAN or packets with a specified MAC address to a monitor port. You can then attach a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity.

PORT TRUNKING Ports can be combined into an aggregate connection. Trunks can be manually set up or dynamically configured using Link Aggregation Control Protocol (LACP – IEEE 802.3-2005). The additional ports dramatically increase the throughput across any connection, and provide redundancy by taking over the load if a port in the trunk should fail. The switch supports up to 8 trunks.

STORM CONTROL Broadcast, multicast and unknown unicast storm suppression prevents traffic from overwhelming the network.When enabled on a port, the level of traffic passing through the port is restricted. If traffic rises above a pre-defined threshold, it will be throttled until the level falls back beneath the threshold.

STATIC ADDRESSES A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be

moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table. Static addresses can be used to provide network security by restricting access for a known host to a specific port.

IP ADDRESS FILTERING

Access to insecure ports can be controlled using DHCP Snooping which filters ingress traffic based on static IP addresses and addresses stored in the DHCP Snooping table. Traffic can also be restricted to specific source IP addresses or source IP/MAC address pairs based on static entries or entries stored in the DHCP Snooping table.

IEEE 802.1D BRIDGE

The switch supports IEEE 802.1D transparent bridging. The address table facilitates data switching by learning addresses, and then filtering or forwarding traffic based on this information. The address table supports up to 8K addresses.

STORE-AND-FORWARD SWITCHING

The switch copies each frame into its memory before forwarding them to another port. This ensures that all frames are a standard Ethernet size and have been verified for accuracy with the cyclic redundancy check (CRC). This prevents bad frames from entering the network and wasting bandwidth.

To avoid dropping frames on congested ports, the switch provides 4 Mbits for frame buffering. This buffer can queue packets awaiting transmission on congested networks.

SPANNING TREE ALGORITHM

The switch supports these spanning tree protocols:

- Spanning Tree Protocol (STP, IEEE 802.1D) – This protocol provides loop detection. When there are multiple physical paths between segments, this protocol will choose a single path and disable all others to ensure that only one route exists between any two stations on the network. This prevents the creation of network loops. However, if the chosen path should fail for any reason, an alternate path will be activated to maintain the connection.

- Rapid Spanning Tree Protocol (RSTP, IEEE 802.1D-2004) – This protocol reduces the convergence time for network topology changes to about 3 to 5 seconds, compared to 30 seconds or more for the older IEEE 802.1D STP standard. It is intended as a complete replacement for STP, but can still interoperate with switches running the older standard by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from attached devices.

- Multiple Spanning Tree Protocol (MSTP, IEEE 802.1D-2004) – This protocol is a direct extension of RSTP. It can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of

each region, and prevents VLAN members from being segmented from the rest of the group (as sometimes occurs with IEEE 802.1D STP).

VIRTUAL LANS

The switch supports up to 255 VLANs. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. The switch supports tagged VLANs based on the IEEE 802.1Q standard. Members of VLAN groups can be dynamically learned via GVRP, or ports can be manually assigned to a specific set of VLANs. This allows the switch to restrict traffic to the VLAN groups to which a user has been assigned. By segmenting your network into VLANs, you can:

- Eliminate broadcast storms which severely degrade performance in a flat network.
- Simplify network management for node changes/moves by remotely configuring VLAN membership for any port, rather than having to manually change the network connection.
- Provide data security by restricting all traffic to the originating VLAN.
- Use private VLANs to restrict traffic to pass only between data ports and the uplink ports, thereby isolating adjacent ports within the same VLAN, and allowing you to limit the total number of VLANs that need to be configured.
- Use protocol VLANs to restrict traffic to specified interfaces based on protocol type.

NOTE: The switch allows 255 user-manageable VLANs. One other VLAN (VLAN ID 4093) is reserved for switch clustering.

TRAFFIC PRIORITIZATION

This switch prioritizes each packet based on the required level of service, using four priority queues with strict or Weighted Round Robin Queuing. It uses IEEE 802.1p and 802.1Q tags to prioritize incoming traffic based on input from the end-station application. These functions can be used to provide independent priorities for delay-sensitive data and best-effort data.

This switch also supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic can be prioritized based on the DSCP field in the IP frame. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

QUALITY OF SERVICE

Differentiated Services (DiffServ) provides policy-based management mechanisms used for prioritizing network resources to meet the requirements of specific traffic types on a per-hop basis. Each packet is classified upon entry into the network based on access lists, IP Precedence

or DSCP values, or VLAN lists. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding.

MULTICAST FILTERING

Specific multicast traffic can be assigned to its own VLAN to ensure that it does not interfere with normal network traffic and to guarantee real-time delivery by setting the required priority level for the designated VLAN. The switch uses IGMP Snooping and Query to manage multicast group registration for IPv4 traffic, and MLD Snooping for IPv6 traffic. It also supports Multicast VLAN Registration (MVR) which allows common multicast traffic, such as television channels, to be transmitted across a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, while preserving security and data isolation for normal traffic.

IEEE 802.1Q TUNNELING (QINQ)

This feature is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting Service Provider VLAN (SPVLAN) tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

SYSTEM DEFAULTS

The switch's system defaults are provided in the configuration file "Factory_Default_Config.cfg." To reset the switch defaults, this file should be set as the startup configuration file.

The following table lists some of the basic system defaults.

Table 2: System Defaults

Function	Parameter	Default
Console Port Connection	Baud Rate	9600 bps
	Data bits	8
	Stop bits	1
	Parity	none
	Local Console Timeout	0 (disabled)

Table 2: System Defaults (Continued)

Function	Parameter	Default
Authentication and Security Measures	Privileged Exec Level	Username "admin" Password "admin"
	Normal Exec Level	Username "guest" Password "guest"
	Enable Privileged Exec from Normal Exec Level	Password "super"
	RADIUS Authentication	Disabled
	TACACS+ Authentication	Disabled
	802.1X Port Authentication	Disabled
	Web Authentication	Disabled
	MAC Authentication	Disabled
	HTTPS	Enabled
	SSH	Disabled
	Port Security	Disabled
	IP Filtering	Disabled
	DHCP Snooping	Disabled
	IP Source Guard	Disabled (all ports)
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
	HTTP Secure Server	Enabled
	HTTP Secure Server Port	443
SNMP	SNMP Agent	Enabled
	Community Strings	"public" (read only) "private" (read/write)
	Traps	Authentication traps: enabled Link-up-down events: enabled
	SNMP V3	View: defaultview Group: public (read only); private (read/write)
Port Configuration	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
Port Trunking	Static Trunks	None
	LACP (all ports)	Disabled
Congestion Control	Rate Limiting	Disabled
	Storm Control	Broadcast: Enabled (64 kbits/sec) Multicast: Disabled Unknown Unicast: Disabled
Address Table	Aging Time	300 seconds

Table 2: System Defaults (Continued)

Function	Parameter	Default
Spanning Tree Algorithm	Status	Enabled, RSTP (Defaults: RSTP standard)
	Edge Ports	Disabled
LLDP	Status	Enabled
Virtual LANs	Default VLAN	1
	PVID	1
	Acceptable Frame Type	All
	Ingress Filtering	Disabled
	Switchport Mode (Egress Mode)	Hybrid: tagged/untagged frames
	GVRP (global)	Disabled
	GVRP (port interface)	Disabled
	QinQ Tunneling	Disabled
Traffic Prioritization	Ingress Port Priority	0
	Queue Mode	WRR
	Queue Weight	Queue: 0 1 2 3 Weight: 1 2 4 8
	Class of Service	Enabled
	IP DSCP Priority	Disabled
IP Settings	Management VLAN	VLAN 1
	IP Address	DHCP assigned
	Subnet Mask	255.255.255.0
	Default Gateway	0.0.0.0
	DHCP	Client: Enabled
	DNS	Proxy service: Disabled
	BOOTP	Disabled
Multicast Filtering	IGMP Snooping (Layer 2)	Snooping: Enabled Querier: Disabled
	Multicast VLAN Registration	Disabled
	MLD Snooping	Disabled
System Log	Status	Enabled
	Messages Logged to RAM	Levels 0-7 (all)
	Messages Logged to Flash	Levels 0-3
SMTP Email Alerts	Event Handler	Enabled (but no server defined)
SNTP	Clock Synchronization	Disabled
NTP	Clock Synchronization	Disabled
Switch Clustering	Status	Enabled
	Commander	Disabled

2 INITIAL SWITCH CONFIGURATION

This chapter includes information on connecting to the switch and basic configuration procedures.

CONNECTING TO THE SWITCH

The switch includes a built-in network management agent. The agent offers a variety of management options, including SNMP, RMON (Groups 1, 2, 3, 9) and a web-based interface. A PC may also be connected directly to the switch for configuration and monitoring via a command line interface (CLI).

NOTE: An IP address for this switch is obtained via DHCP by default. To change this address, see "Setting an IP Address."

CONFIGURATION OPTIONS

The switch's HTTP web agent allows you to configure switch parameters, monitor port connections, and display statistics using a standard web browser such as Internet Explorer 5.x or above, Netscape 6.2 or above, and Mozilla Firefox 2.0.0.0 or above. The switch's web management interface can be accessed from any computer attached to the network.

The CLI program can be accessed by a direct connection to the RS-232 serial console port on the switch, or remotely by a Telnet or Secure Shell (SSH) connection over the network.

The switch's management agent also supports SNMP (Simple Network Management Protocol). This SNMP agent permits the switch to be managed from any system in the network using network management software.

The switch's web interface, console interface, and SNMP agent allow you to perform management functions such as those shown below:

- Set user names and passwords
- Set an IP interface for a management VLAN
- Configure SNMP parameters
- Enable/disable any port
- Set the speed/duplex mode for any port

- Configure the bandwidth of any port by limiting input or output rates
- Control port access through IEEE 802.1X security or static address filtering
- Filter packets using Access Control Lists (ACLs)
- Configure up to 255 IEEE 802.1Q VLANs
- Enable GVRP automatic VLAN registration
- Configure IGMP multicast filtering
- Upload and download system firmware or configuration files via HTTP (using the web interface) or FTP/TFTP (using the command line or web interface)
- Configure Spanning Tree parameters
- Configure Class of Service (CoS) priority queuing
- Configure static or LACP trunks (up to 8)
- Enable port mirroring
- Set storm control on any port for excessive broadcast, multicast, or unknown unicast traffic
- Display system information and statistics

REQUIRED CONNECTIONS

The switch provides an RS-232 serial port that enables a connection to a PC or terminal for monitoring and configuring the switch. A null-modem console cable is provided with the switch.

Attach a VT100-compatible terminal, or a PC running a terminal emulation program to the switch. You can use the console cable provided with this package, or use a null-modem cable that complies with the wiring assignments shown in the Installation Guide.

To connect a terminal to the console port, complete the following steps:

1. Connect the console cable to the serial port on a terminal, or a PC running terminal emulation software, and tighten the captive retaining screws on the DB-9 connector.
2. Connect the other end of the cable to the RS-232 serial port on the switch.
3. Make sure the terminal emulation software is set as follows:
   - Select the appropriate serial port (COM port 1 or COM port 2).
   - Set the baud rate to 9600 bps.

- Set the data format to 8 data bits, 1 stop bit, and no parity.
- Set flow control to none.
- Set the emulation mode to VT100.
- When using HyperTerminal, select Terminal keys, not Windows keys.

NOTE: Once you have set up the terminal correctly, the console login screen will be displayed.

For a description of how to use the CLI, see "Using the Command Line Interface." For a list of all the CLI commands and detailed information on using the CLI, refer to "CLI Command Groups."

REMOTE CONNECTIONS

Prior to accessing the switch's onboard agent via a network connection, you must first configure it with a valid IP address, subnet mask, and default gateway using a console connection, or DHCP protocol.

The IP address for this switch is obtained via DHCP by default. To manually configure this address or enable dynamic address assignment via DHCP, see "Setting an IP Address."

NOTE: This switch supports four concurrent Telnet or SSH sessions.

After configuring the switch's IP parameters, you can access the onboard configuration program from anywhere within the attached network. The command-line interface can be accessed using Telnet from any computer attached to the network. The switch can also be managed by any computer using a web browser (Internet Explorer 5.0 or above, Netscape 6.2 or above, or Mozilla Firefox 2.0.0.0 or above), or from a network computer using SNMP network management software.

The onboard program only provides access to basic configuration functions. To access the full range of SNMP management functions, you must use SNMP-based network management software.

BASIC CONFIGURATION

CONSOLE CONNECTION

The CLI program provides two different command levels — normal access level (Normal Exec) and privileged access level (Privileged Exec). The commands available at the Normal Exec level are a limited subset of those available at the Privileged Exec level and allow you to only display information and use basic utilities. To fully configure the switch parameters, you must access the CLI at the Privileged Exec level.

Access to both CLI levels are controlled by user names and passwords. The switch has a default user name and password for each level. To log into the CLI at the Privileged Exec level using the default user name and password, perform these steps:

1. To initiate your console connection, press <Enter>. The "User Access Verification" procedure starts.
2. At the User Name prompt, enter "admin."
3. At the Password prompt, also enter "admin." (The password characters are not displayed on the console screen.)
4. The session is opened and the CLI displays the "Console#" prompt indicating you have access at the Privileged Exec level.

SETTING PASSWORDS

If this is your first time to log into the CLI program, you should define new passwords for both default user names using the "username" command, record them and put them in a safe place.

Passwords can consist of up to 32 alphanumeric characters and are case sensitive. To prevent unauthorized access to the switch, set the passwords as follows:

1. Open the console interface with the default user name and password "admin" to access the Privileged Exec level.
2. Type "configure" and press <Enter>.
3. Type "username guest password 0 *password*," for the Normal Exec level, where *password* is your new password. Press <Enter>.
4. Type "username admin password 0 *password*," for the Privileged Exec level, where *password* is your new password. Press <Enter>.

```
Username: admin
Password:

 CLI session with the ES3528M* is opened.
 To end the CLI session, enter [Exit].
```

```
Console#configure
Console(config)#username guest password 0 [password]
Console(config)#username admin password 0 [password]
Console(config)#
```

* This manual covers both the ES3528M and ES3552M. Other than the number of ports, there are no other significant differences. Therefore all of the screen display examples are based on the ES3528M.

SETTING AN IP ADDRESS

You must establish IP address information for the switch to obtain management access through the network. This can be done in either of the following ways:

- **Manual** — You have to input the information, including IP address and subnet mask. If your management station is not in the same IP subnet as the switch, you will also need to specify the default gateway router.
- **Dynamic** — The switch can send IP configuration requests to BOOTP or DHCP address allocation servers on the network.

MANUAL CONFIGURATION

You can manually assign an IP address to the switch. You may also need to specify a default gateway that resides between this device and management stations that exist on another network segment. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.

NOTE: The IP address for this switch is obtained via DHCP by default.

Before you can assign an IP address to the switch, you must obtain the following information from your network administrator:

- IP address for the switch
- Network mask for this network
- Default gateway for the network

To assign an IP address to the switch, complete the following steps

1. From the Global Configuration mode prompt, type "interface vlan 1" to access the interface-configuration mode. Press <Enter>.
2. Type "ip address *ip-address netmask*," where "ip-address" is the switch IP address and "netmask" is the network mask for the network. Press <Enter>.
3. Type "exit" to return to the global configuration mode prompt. Press <Enter>.

4. To set the IP address of the default gateway for the network to which the switch belongs, type "ip default-gateway *gateway*," where "gateway" is the IP address of the default gateway. Press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254
```

DYNAMIC CONFIGURATION

Obtaining an IPv4 Address

If you select the "bootp" or "dhcp" option, the system will immediately start broadcasting service requests. IP will be enabled but will not function until a BOOTP or DHCP reply has been received. Requests are broadcast every few minutes using exponential backoff until IP configuration information is obtained from a BOOTP or DHCP server. BOOTP and DHCP values can include the IP address, subnet mask, and default gateway. If the DHCP/BOOTP server is slow to respond, you may need to use the "ip dhcp restart" command to re-start broadcasting service requests.

Note that the "ip dhcp restart" command can be used to start broadcasting service requests for any VLAN configured to obtain address assignments through BOOTP or DHCP. It may be necessary to use this command when DHCP is configured on a VLAN, and the member ports which were previously shut down are now enabled.

If the "bootp" or "dhcp" option is saved to the startup-config file (step 6), then the switch will start broadcasting service requests as soon as it is powered on.

To automatically configure the switch by communicating with BOOTP or DHCP address allocation servers on the network, complete the following steps:

1. From the Global Configuration mode prompt, type "interface vlan 1" to access the interface-configuration mode. Press <Enter>.

2. At the interface-configuration mode prompt, use one of the following commands:

   - To obtain IP settings via DHCP, type "ip address dhcp" and press <Enter>.

   - To obtain IP settings via BOOTP, type "ip address bootp" and press <Enter>.

3. Type "end" to return to the Privileged Exec mode. Press <Enter>.

4. Wait a few minutes, and then check the IP configuration settings by typing the "show ip interface" command. Press <Enter>.

5. Then save your configuration changes by typing "copy running-config startup-config." Enter the startup file name and press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#end
Console#show ip interface
 IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
 and address mode: DHCP
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.
```

DOWNLOADING A CONFIGURATION FILE REFERENCED BY A DHCP SERVER

Information passed on to the switch from a DHCP server may also include a configuration file to be downloaded and the TFTP servers where that file can be accessed. If the Factory Default Configuration file is used to provision the switch at startup, in addition to requesting IP configuration settings from the DHCP server, it will also ask for the name of a bootup configuration file and TFTP servers where that file is stored.

If the switch receives information that allows it to download the remote bootup file, it will save this file to a local buffer, and then restart the provision process.

Note the following DHCP client behavior:

- The bootup configuration file received from a TFTP server is stored on the switch with the original file name. If this file name already exists in the switch, the file is overwritten.
- If the name of the bootup configuration file is the same as the Factory Default Configuration file, the download procedure will be terminated, and the switch will not send any further DHCP client requests.
- If the switch fails to download the bootup configuration file based on information passed by the DHCP server, it will not send any further DHCP client requests.
- If the switch does not receive a DHCP response prior to completing the bootup process, it will continue to send a DHCP client request once a minute. These requests will only be terminated if the switch's address is manually configured, but will resume if the address mode is set back to DHCP.

To successfully transmit a bootup configuration file to the switch the DHCP daemon (using a Linux based system for this example) must be configured with the following information:

- Options 60, 66 and 67 statements can be added to the daemon's configuration file.

Table 3: Options 60, 66 and 67 Statements

Option	Statement	
	Keyword	Parameter
60	vendor-class-identifier	a string indicating the vendor class identifier
66	tftp-server-name	a string indicating the tftp server name
67	bootfile-name	a string indicating the bootfile name

- By default, DHCP option 66/67 parameters are not carried in a DHCP server reply. To ask for a DHCP reply with option 66/67 information, the DHCP client request sent by this switch includes a "parameter request list" asking for this information. Besides, the client request also includes a "vendor class identifier" that allows the DHCP server to identify the device, and select the appropriate configuration file for download. This information is included in Option 55 and 124.

Table 4: Options 55 and 124 Statements

Option	Statement	
	Keyword	Parameter
55	dhcp-parameter-request-list	a list of parameters, separated by ','
124	vendor-class-identifier	a string indicating the vendor class identifier

The following configuration examples are provided for a Linux-based DHCP daemon (dhcpd.conf file). The server will reply with Options 66/67 encapsulated in Option 43. Note that in the "Vendor class two" section, the server still sends Option 43 telling the switch to download the test2 configuration file from the server 192.168.255.101.

```
ddns-update-style ad-hoc;

default-lease-time 600;
max-lease-time 7200;

log-facility local7;

server-name "Server1";
Server-identifier 192.168.255.250;
#option 43 with encapsulated option 66, 67
 option space dynamicProvision code width 1 length 1 hash size 2;
 option dynamicProvision.tftp-server-name code 66 = text;
 option dynamicProvision.bootfile-name code 67 = text;

subnet 192.168.255.0 netmask 255.255.255.0 {
  range 192.168.255.160 192.168.255.200;
  option routers 192.168.255.101;
```

```
  option tftp-server-name "192.168.255.100";#Default Option 66
  option bootfile-name "bootfile";           #Default Option 67
}

class "Option66,67_1" {                 #DHCP Option 60 Vendor class
one
 match if option vendor-class-identifier = "ES3552M-PoE";
 option dhcp-parameter-request-list 1,43,66,67;
#option 43
 option vendor-class-information code 43 = encapsulate
   dynamicProvision;
#option 66 encapsulated in option 43
 option vendor-class-information.tftp-server-name "192.168.255.100";
#option 67 encapsulated in option 43
    option vendor-class-information.bootfile-name "test1"
}

class "Option66,67_2" {                #DHCP Option 60 Vendor class
two
  match if option vendor-class-identifier = "ES3552M-PoE";
  option dhcp-parameter-request-list 1,43,66,67;
  option tftp-server-name "192.168.255.101";
  option bootfile-name "test2";
}
```

NOTE: Use “ES3552M-PoE” for the vendor-class-identifier in the dhcpd.conf file.

ENABLING SNMP MANAGEMENT ACCESS

The switch can be configured to accept management commands from Simple Network Management Protocol (SNMP) applications. You can configure the switch to respond to SNMP requests or generate SNMP traps.

When SNMP management stations send requests to the switch (either to return information or to set a parameter), the switch provides the requested data or sets the specified parameter. The switch can also be configured to send information to SNMP managers (without being requested by the managers) through trap messages, which inform the manager that certain events have occurred.

The switch includes an SNMP agent that supports SNMP version 1, 2c, and 3 clients. To provide management access for version 1 or 2c clients, you must specify a community string. The switch provides a default MIB View (i.e., an SNMPv3 construct) for the default “public” community string that provides read access to the entire MIB tree, and a default view for the “private” community string that provides read/write access to the entire MIB tree. However, you may assign new views to version 1 or 2c community strings that suit your specific security requirements (see "Setting SNMPv3 Views").

COMMUNITY STRINGS (FOR SNMP VERSION 1 AND 2C CLIENTS)

Community strings are used to control management access to SNMP version 1 and 2c stations, as well as to authorize SNMP stations to receive trap messages from the switch. You therefore need to assign community strings to specified users, and set the access level.

The default strings are:

- **public** - with read-only access. Authorized management stations are only able to retrieve MIB objects.
- **private** - with read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

To prevent unauthorized access to the switch from SNMP version 1 or 2c clients, it is recommended that you change the default community strings.

To configure a community string, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type "snmp-server community *string mode*," where "string" is the community access string and "mode" is **rw** (read/write) or **ro** (read only). Press <Enter>. (Note that the default mode is read only.)
2. To remove an existing string, simply type "no snmp-server community *string*," where "string" is the community access string to remove. Press <Enter>.

```
Console(config)#snmp-server community admin rw
Console(config)#snmp-server community private
Console(config)#
```

NOTE: If you do not intend to support access to SNMP version 1 and 2c clients, we recommend that you delete both of the default community strings. If there are no community strings, then SNMP management access from SNMP v1 and v2c clients is disabled.

TRAP RECEIVERS

You can also specify SNMP stations that are to receive traps from the switch. To configure a trap receiver, use the "snmp-server host" command. From the Privileged Exec level global configuration mode prompt, type:

"snmp-server host *host-address community-string*
[version {1 | 2c | 3 {auth | noauth | priv}}]"

where "host-address" is the IP address for the trap receiver, "community-string" specifies access rights for a version 1/2c host, or is the user name of a version 3 host, "version" indicates the SNMP client version, and "auth | noauth | priv" means that authentication, no authentication, or

authentication and privacy is used for v3 clients. Then press <Enter>. For a more detailed description of these parameters, see "snmp-server host." The following example creates a trap host for each type of SNMP client.

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#snmp-server host 10.1.19.98 robin version 2c
Console(config)#snmp-server host 10.1.19.34 barbie version 3 auth
Console(config)#
```

CONFIGURING ACCESS FOR SNMP VERSION 3 CLIENTS

To configure management access for SNMPv3 clients, you need to first create a view that defines the portions of MIB that the client can read or write, assign the view to a group, and then assign the user to a group. The following example creates one view called "mib-2" that includes the entire MIB-2 tree branch, and then another view that includes the IEEE 802.1D bridge MIB. It assigns these respective read and read/write views to a group call "r&d" and specifies group authentication via MD5 or SHA. In the last step, it assigns a v3 user to this group, indicating that MD5 will be used for authentication, provides the password "greenpeace" for authentication, and the password "einstien" for encryption.

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included
Console(config)#snmp-server view 802.1d 1.3.6.1.2.1.17 included
Console(config)#snmp-server group r&d v3 auth mib-2 802.1d
Console(config)#snmp-server user steve group r&d v3 auth md5 greenpeace priv
  des56 einstien
Console(config)#
```

For a more detailed explanation on how to configure the switch for access from SNMPv3 clients, refer to "Simple Network Management Protocol," or refer to the specific CLI commands for SNMP starting on page 527.

MANAGING SYSTEM FILES

The switch's flash memory supports three types of system files that can be managed by the CLI program, web interface, or SNMP. The switch's file system allows files to be uploaded and downloaded, copied, deleted, and set as a start-up file.

The types of files are:

- **Configuration** — This file type stores system configuration information and is created when configuration settings are saved. Saved configuration files can be selected as a system start-up file or can be uploaded via FTP/TFTP to a server for backup. The file named "Factory_Default_Config.cfg" contains all the system default settings and cannot be deleted from the system. If the system is booted with the factory default settings, the switch will also create a file named "startup1.cfg" that contains system settings for switch initialization, including information about the unit identifier, and MAC address for the

switch. The configuration settings from the factory defaults configuration file are copied to this file, which is then used to boot the switch. See "Saving or Restoring Configuration Settings" for more information.

- **Operation Code** — System software that is executed after boot-up, also known as run-time code. This code runs the switch operations and provides the CLI and web management interfaces. See "Managing System Files" for more information.

- **Diagnostic Code** — Software that is run during system boot-up, also known as POST (Power On Self-Test).

Due to the size limit of the flash memory, the switch supports only two operation code files. However, you can have as many diagnostic code files and configuration files as available flash memory space allows. The switch has a total of 16 Mbytes of flash memory for system files.

In the system flash memory, one file of each type must be set as the start-up file. During a system boot, the diagnostic and operation code files set as the start-up file are run, and then the start-up configuration file is loaded.

Note that configuration files should be downloaded using a file name that reflects the contents or usage of the file settings. If you download directly to the running-config, the system will reboot, and the settings will have to be copied from the running-config to a permanent file.

SAVING OR RESTORING CONFIGURATION SETTINGS

Configuration commands only modify the running configuration file and are not saved when the switch is rebooted. To save all your configuration changes in nonvolatile storage, you must copy the running configuration file to the start-up configuration file using the "copy" command.

New startup configuration files must have a name specified. File names on the switch are case-sensitive, can be from 1 to 31 characters, must not contain slashes (\ or /), and the leading letter of the file name must not be a period (.). (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

There can be more than one user-defined configuration file saved in the switch's flash memory, but only one is designated as the "startup" file that is loaded when the switch boots. The **copy running-config startup-config** command always sets the new file as the startup file. To select a previously saved configuration file, use the **boot system config:**<*filename*> command.

The maximum number of saved configuration files depends on available flash memory with each configuration file normally requiring less than 20 kbytes. The amount of available flash memory can be checked by using the **dir** command.

To save the current configuration settings, enter the following command:

1. From the Privileged Exec mode prompt, type "copy running-config startup-config" and press <Enter>.

2. Enter the name of the start-up file. Press <Enter>.

```
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.
```

To restore configuration settings from a backup server, enter the following command:

1. From the Privileged Exec mode prompt, type "copy tftp startup-config" and press <Enter>.
2. Enter the address of the TFTP server. Press <Enter>.
3. Enter the name of the startup file stored on the server. Press <Enter>.
4. Enter the name for the startup file on the switch. Press <Enter>.

```
Console#copy file startup-config
Console#copy tftp startup-config
TFTP server IP address: 192.168.0.4
Source configuration file name: startup-rd.cfg
Startup configuration file name [startup1.cfg]:

Success.
Console#
```

SECTION II

WEB CONFIGURATION

This section describes the basic switch features, along with a detailed description of how to configure each feature via a web browser.

This section includes these chapters:

3 USING THE WEB INTERFACE

This switch provides an embedded HTTP web agent. Using a web browser you can configure the switch and view statistics to monitor network activity. The web agent can be accessed by any computer on the network using a standard web browser (Internet Explorer 5.0 or above, Netscape 6.2 or above, or Mozilla Firefox 2.0.0.0 or above).

NOTE: You can also use the Command Line Interface (CLI) to manage the switch over a serial connection to the console port or via Telnet. For more information on using the CLI, refer to "Using the Command Line Interface."

CONNECTING TO THE WEB INTERFACE

Prior to accessing the switch from a web browser, be sure you have first performed the following tasks:

1. Configure the switch with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection, BOOTP or DHCP protocol. (See "Setting an IP Address.")
2. Set user names and passwords using an out-of-band serial connection. Access to the web agent is controlled by the same user names and passwords as the onboard configuration program. (See "Setting Passwords.")
3. After you enter a user name and password, you will have access to the system configuration program.

NOTE: You are allowed three attempts to enter the correct password; on the third failed attempt the current connection is terminated.

NOTE: If you log into the web interface as guest (Normal Exec level), you can view the configuration settings or change the guest password. If you log in as "admin" (Privileged Exec level), you can change the settings on any page.

NOTE: If the path between your management station and this switch does not pass through any device that uses the Spanning Tree Algorithm, then you can set the switch port attached to your management station to fast forwarding (i.e., enable Admin Edge Port) to improve the switch's response time to management commands issued through the web interface. See "Configuring Interface Settings for STA."

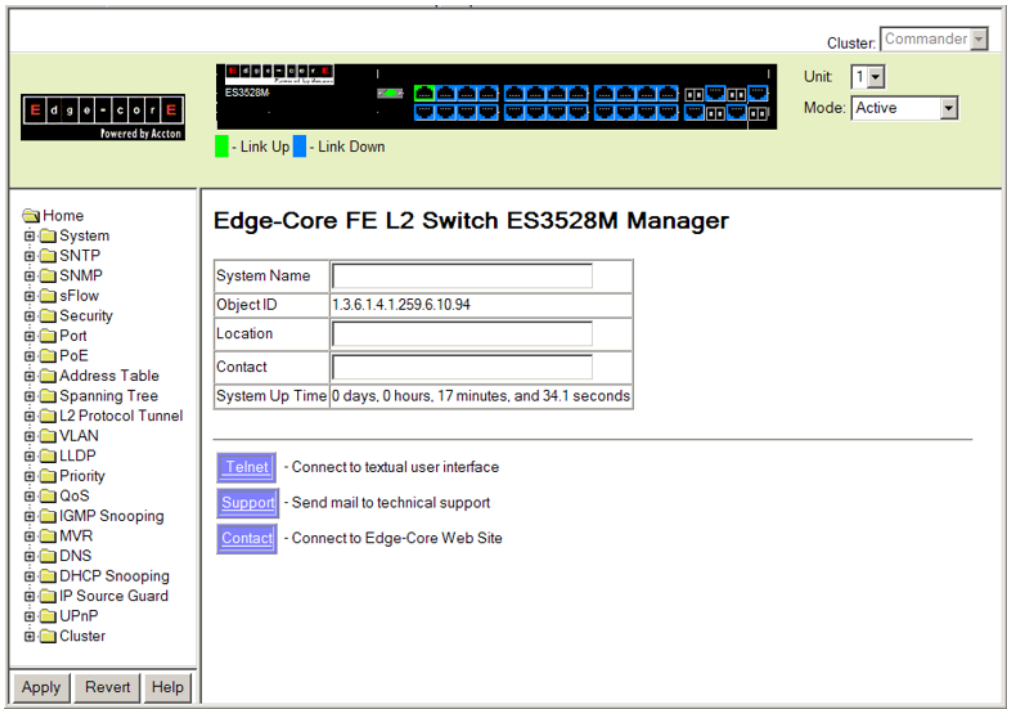
NAVIGATING THE WEB BROWSER INTERFACE

To access the web-browser interface you must first enter a user name and password. The administrator has Read/Write access to all configuration parameters and statistics. The default user name and password for the administrator is "admin."

HOME PAGE

When your web browser connects with the switch's web agent, the home page is displayed as shown below. The home page displays the Main Menu on the left side of the screen and System Information on the right side. The Main Menu links are used to navigate to other menus, and display configuration parameters and statistics.

Figure 1: Home Page



NOTE: The examples in this chapter are based on the ES3528M. Other than the number of fixed ports, there are no other differences between the ES3528M and ES3552M. The panel graphics for both switch types are shown on the following page.

NOTE: You can open a connection to the manufacturer's web site by clicking on the Edge-core logo.

CONFIGURATION OPTIONS

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the Apply button to confirm the new setting. The following table summarizes the web page configuration buttons.

Table 5: Web Page Configuration Buttons

Button	Action
Apply	Sets specified values to the system.
Revert	Cancels specified values and restores current values prior to pressing "Apply."
Help	Links directly to web help.

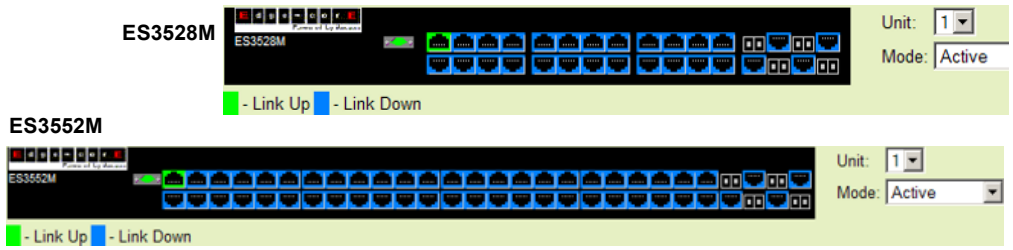
NOTE: To ensure proper screen refresh, be sure that Internet Explorer 5.x is configured as follows: Under the menu "Tools / Internet Options / General / Temporary Internet Files / Settings," the setting for item "Check for newer versions of stored pages" should be "Every visit to the page."

NOTE: When using Internet Explorer 5.0, you may have to manually refresh the screen after making configuration changes by pressing the browser's refresh button.

PANEL DISPLAY

The web agent displays an image of the switch's ports. The Mode can be set to display different information for the ports, including Active (i.e., up or down), Duplex (i.e., half or full duplex), or Flow Control (i.e., with or without flow control).

Figure 2: Front Panel Indicators



MAIN MENU Using the onboard web agent, you can define system parameters, manage and control the switch, and all its ports, or monitor network conditions. The following table briefly describes the selections available from this program.

Table 6: Switch Main Menu

Menu	Description	Page
System		
System Information	Provides basic system description, including contact information	96
Switch Information	Shows the number of ports, hardware version, power status, and firmware version numbers	97
Bridge Extension Configuration	Shows the bridge extension parameters	99
IP Configuration	Sets the IP address for management access	100
Jumbo Frames	Enables jumbo frame packets.	105
Resource		
CPU Status	Displays information on CPU utilization; also sets thresholds for CPU utilization alarm	106
Memory Status	Displays information on memory utilization; also sets thresholds for memory utilization alarm	107
File Management		108
Automatic Operation Code Upgrade	Automatically upgrades operation code if a newer version is found on the server	108
Copy Operation	Allows the transfer and copying of files	112
HTTP Upgrade	Copies operation code or configuration files from management station to the switch	116
HTTP Download	Copies operation code or configuration files from the switch to the management station	116
Delete	Allows deletion of files from the flash memory	118
Set Start-Up	Sets the startup file	118
Line		
Console	Sets console port connection parameters	119
Telnet	Sets Telnet connection parameters	121
Log		122
Logs	Stores and displays error messages	122
System Logs	Sends error messages to a logging process	122
Remote Logs	Configures the logging of messages to a remote logging process	124
SMTP	Sends an SMTP client message to a participating server.	126
Reset	Restarts the switch immediately, or after a specified delay	127
SNTP	Simple Network Time Protocol	
Current Time	Manually sets the current time	129
Configuration	Configures SNTP and NTP client settings, including broadcast mode, authentication parameters or a specified list of servers	130
Time Zone	Sets the local time zone for the system clock	133

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Summer Time	Configures summer time settings	134
SNMP	Simple Network Management Protocol	143
Configuration	Configures community strings and related trap functions	145
Port Configuration	Enables traps when changes occur for dynamic addresses in the MAC address table for a port	150
Trunk Configuration	Enables traps when changes occur for dynamic addresses in the MAC address table for a trunk	150
Agent Status	Enables or disables SNMP Agent Status	151
SNMPv3		
Engine ID	Sets the SNMP v3 engine ID on this switch	152
Remote Engine ID	Sets the SNMP v3 engine ID for a remote device	153
Users	Configures SNMP v3 users on this switch	154
Remote Users	Configures SNMP v3 users from a remote device	155
Groups	Configures SNMP v3 groups	158
Views	Configures SNMP v3 views	162
sFlow	Samples traffic flows, and forwards data to designated collector	165
Configuration	Globally enables flow sampling, enables sampling per port, and sets the sampling rate per port	166
Port Configuration	Sets destination parameters, payload parameters, and sampling interval	167
Security		169
User Accounts	Configures user names, passwords, and access levels	170
Authentication Settings	Configures authentication sequence – local, RADIUS, TACACS	171
Encryption Key	Configures RADIUS and TACACS encryption key settings	174
AAA	Authentication, Authorization and Accounting	176
RADIUS Group Settings	Defines the configured RADIUS servers to use for accounting, and sets the priority sequence	177
TACACS+ Group Settings	Defines the configured TACACS+ servers to use for accounting, and sets the priority sequence	178
Accounting	Enables accounting of requested services for billing or security purposes	
Settings	Configures accounting of requested services for billing or security purposes	179
Periodic Update	Specifies the interval at which the local accounting service updates information to the accounting server	180
802.1X Port Settings	Applies the specified accounting method to an interface	181
Command Privileges	Specifies a method name to apply to commands entered at specific CLI privilege levels	182
Exec Settings	Specifies console or Telnet authentication method	183
Summary	Displays configured accounting methods and statistics	183

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Authorization	Enables authorization of requested services	
Settings	Configures authorization for various service types	185
EXEC Settings	Specifies console or Telnet authorization method	186
Summary	Displays authorization information	187
HTTPS Settings	Configures secure HTTP settings; replaces the default secure-site certificate	188
SSH	Secure Shell	191
Settings	Configures Secure Shell server settings	194
Host-Key Settings	Generates the host key pair (public and private)	195
User Public-Key Settings	Imports user public keys from TFTP server	197
Port Security	Configures per port security, including status, response for security breach, and maximum allowed MAC addresses	198
802.1X	Port authentication	200
Information	Displays global configuration settings	202
Configuration	Enables authentication and EAPOL pass-through	202
Authenticator Port Configuration	Sets authentication parameters for individual ports	203
Supplicant Port Configuration	Sets port settings for supplicant requests issued from a port to an authenticator on another device	206
Authenticator Statistics	Displays dot1x authenticator statistics for the selected port	208
Supplicant Statistics	Displays dot1x supplicant statistics for the selected port	209
Web Authentication	Allows authentication and access to the network when 802.1X or Network Access authentication are infeasible or impractical	210
Configuration	Configures general protocol settings	211
Port Configuration	Enables Web Authentication for individual ports	212
Port Information	Displays status information for individual ports	213
Re-authentication	Forces a host to re-authenticate itself immediately	213
Network Access	MAC address-based network access authentication	215
Configuration	Enables aging for authenticated MAC addresses, and sets the time period after which a connected MAC address must be reauthenticated	217
Port Configuration	Enables MAC authentication on a port; sets the maximum number of address that can be authenticated, the guest VLAN, dynamic VLAN and dynamic QoS	218
Port Link Detection Configuration	Configures detection of changes in link status, and the response (i.e., send trap or shut down port)	220
MAC Address Information	Shows the authenticated MAC address list	221
MAC Filter Configuration	Specifies MAC addresses exempt from authentication	223
ACL	Access Control Lists	224
Configuration	Configures packet filtering based on IP or MAC addresses	225
Port Binding	Binds a port to the specified ACL	236
TCAM Utilization	Shows utilization parameters for TCAM	237

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
ARP Inspection	Validates the MAC-to-IP address bindings in ARP packets	238
Configuration	Enables inspection globally, configures validation of additional address components, and sets the log rate for packet inspection	239
VLAN Configuration	Enables ARP inspection on specified VLANs	241
Port Configuration	Sets the trust mode for ports, and sets the rate limit for packet inspection	243
Log Information	Displays information on results of inspection process	244
Statistics	Displays statistics on the inspection process	245
IP Filter	Sets IP addresses of clients allowed management access via the web, SNMP, and Telnet	246
Port		261
Port Information	Displays port connection status	261
Trunk Information	Displays trunk connection status	261
Port Configuration	Configures port connection settings	262
Trunk Configuration	Configures trunk connection settings	262
Trunk Membership	Specifies ports to group into static trunks	266
LACP	Link Aggregation Control Protocol	
Configuration	Allows ports to dynamically join trunks	268
Aggregation Port	Configures parameters for link aggregation group members	269
Aggregation Group	Configures the administration key for specific LACP groups	271
Port Counters Information	Displays statistics for LACP protocol messages	272
Port Internal Information	Displays configuration settings and operational state for the local side of a link aggregation	273
Port Neighbors Information	Displays configuration settings and operational state for the remote side of a link aggregation	275
Port Broadcast Control	Sets the broadcast storm threshold for each port	277
Trunk Broadcast Control	Sets the broadcast storm threshold for each trunk	277
Port Multicast Control	Sets the multicast storm threshold for each port	278
Trunk Multicast Control	Sets the multicast storm threshold for each trunk	278
Port Unknown Unicast Control	Sets the unknown unicast storm threshold for each port	279
Trunk Unknown Unicast Control	Sets the unknown unicast storm threshold for each trunk	279
Mirror Port Configuration	Sets the source and target ports for mirroring	281
MAC Mirror Configuration	Sets a MAC address for packets to be mirrored from any source port other than the target port to the specified destination port	282
Rate Limit		284
Input Port Configuration	Sets the input rate limit for each port	284
Input Trunk Configuration	Sets the input rate limit for each trunk	284
Output Port Configuration	Sets the output rate limit for ports	284
Output Trunk Configuration	Sets the output rate limit for trunks	284

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Port VLAN Trunking	Allows unknown VLAN groups to pass through the specified port	285
Trunk VLAN Trunking	Allows unknown VLAN groups to pass through the specified trunk	285
Cable Test	Performs cable diagnostics for selected port to diagnose any cable faults (short, open etc.) and report the cable length	287
Port Statistics	Shows Interface, Etherlike, and RMON port statistics	288
Address Table		293
Static Addresses	Configures static entries in the address table	293
Dynamic Addresses	Displays dynamic entries in the address table	295
Address Aging	Sets timeout for dynamically learned entries	296
Spanning Tree		299
Port Loopback Detection	Configures Port Loopback Detection parameters	302
Trunk Loopback Detection	Configures Trunk Loopback Detection parameters	302
STA	Spanning Tree Algorithm	302
Information	Displays STA values used for the bridge	303
Configuration	Configures global bridge settings for STP, RSTP and MSTP	305
Port Information	Displays individual port settings for STA	309
Trunk Information	Displays individual trunk settings for STA	309
Port Configuration	Configures individual port settings for STA	312
Trunk Configuration	Configures individual trunk settings for STA	312
Port Edge Port Configuration	Sets an interface to function as an edge port, either manually or by automatic configuration	315
Trunk Edge Port Configuration	Sets an interface to function as an edge port, either manually or by automatic configuration	315
MSTP	Multiple Spanning Tree Protocol	
VLAN Configuration	Configures priority and VLANs for a spanning tree instance	317
Port Information	Displays port settings for a specified MST instance	319
Trunk Information	Displays trunk settings for a specified MST instance	319
Port Configuration	Configures port settings for a specified MST instance	320
Trunk Configuration	Configures trunk settings for a specified MST instance	320
L2 Protocol Tunnel	Passes specified protocol packet types belonging to the same customer transparently across a service provider's network	323
Configuration	Configures the destination address for PDU tunneling	323
Port Configuration	Enables Layer 2 Protocol Tunneling for the specified protocol	324
Trunk Configuration	Enables Layer 2 Protocol Tunneling for the specified protocol	324
VLAN	Virtual LAN	327
802.1Q VLAN	IEEE 802.1Q VLANs	327
GVRP Status	Enables GVRP VLAN registration protocol globally	331
Basic Information	Displays information on the VLAN type supported by this switch	331

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Current Table	Shows the current port members of each VLAN and whether or not the port is tagged or untagged	332
Static List	Used to create or remove VLAN groups	333
Static Table	Modifies the settings for an existing VLAN	334
Static Membership by Port	Configures membership type for interfaces, including tagged, untagged or forbidden	336
Port Configuration	Specifies default PVID, VLAN attributes; as well as GVRP status and timers per port	337
Trunk Configuration	Specifies default PVID, VLAN attributes; as well as GVRP status and timers per trunk	337
Tunnel Configuration	Enables 802.1Q (QinQ) Tunneling	343
Tunnel Port Configuration	Sets the tunnel mode for an interface	344
Tunnel Trunk Configuration	Sets the tunnel mode for an interface	344
Traffic Segmentation	Configures traffic segmentation for different client sessions based on specified downlink and uplink ports	345
Status	Enables traffic segmentation, and blocks or forwards traffic between uplink ports assigned to different client sessions	345
Session Configuration	Creates a client session, and assigns the downlink and uplink ports to service the traffic	346
Private VLAN		347
Information	Displays Private VLAN feature information	348
Configuration	This page is used to create/remove primary or community VLANs	349
Association	Each community VLAN must be associated with a primary VLAN	350
Port Information	Shows VLAN port type, and associated primary or secondary VLANs	350
Port Configuration	Sets the private VLAN interface type, and associates the interfaces with a private VLAN	352
Trunk Information	Shows VLAN port type, and associated primary or secondary VLANs	350
Trunk Configuration	Sets the private VLAN interface type, and associates the interfaces with a private VLAN	352
Protocol VLAN		353
Configuration	Creates a protocol group, specifying the supported protocols	354
System Configuration	Maps a protocol group to a VLAN	355
VLAN Mirror Configuration	Mirrors traffic from one or more source VLANs to a target port	356
IP Subnet VLAN		358
Configuration	Maps IP subnet traffic to a VLAN	358
MAC-based VLAN		359
Configuration	Maps traffic with specified source MAC address to a VLAN	359

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
LLDP	Link Layer Discovery Protocol	361
Configuration	Configures global LLDP timing parameters	362
Port Configuration	Sets the message transmission mode; enables SNMP notification; and sets the LLDP attributes to advertise for ports	364
Trunk Configuration	Sets the message transmission mode; enables SNMP notification; and sets the LLDP attributes to advertise for trunks	364
Local Information	Displays general information about the local device	367
Remote Port Information	Displays information about a remote device connected to a port on this switch	369
Remote Trunk Information	Displays information about a remote device connected to a trunk on this switch	369
Remote Information Details	Displays detailed information about a remote device connected to this switch	370
Device Statistics	Displays statistics for all connected remote devices	372
Device Statistics Details	Displays statistics for remote devices on a selected port or trunk	373
Priority		375
Default Port Priority	Sets the default priority for each port	375
Default Trunk Priority	Sets the default priority for each trunk	375
Traffic Classes	Maps IEEE 802.1p priority tags to output queues	376
Traffic Classes Status	Enables/disables traffic class priorities (not implemented)	NA
Queue Mode	Sets queue mode to strict priority or Weighted Round-Robin	378
Queue Scheduling	Configures Weighted Round Robin queueing	379
IP DSCP Priority Status	Globally selects DSCP Priority, or disables it.	380
IP DSCP Priority	Sets IP Differentiated Services Code Point priority, mapping a DSCP tag to a class-of-service value	381
QoS	Quality of Service	383
DiffServ	Configure QoS classification criteria and service policies	383
Class Map	Creates a class map for a type of traffic	384
Policy Map	Creates a policy map for multiple interfaces	387
Service Policy	Applies a policy map defined to an ingress port	391
VoIP Traffic Setting		393
Configuration	Configures auto-detection of VoIP traffic, sets the Voice VLAN, nd VLAN aging time	394
Port Configuration	Configures VoIP traffic settings for ports, including the way in which a port is added to the Voice VLAN, filtering of non-VoIP packets, the method of detecting VoIP traffic, and the priority assigned to the voice traffic	395
OUI Configuration	Maps the OUI in the source MAC address of ingress packets to the VoIP device manufacturer	397
IGMP Snooping		399
IGMP Configuration	Enables multicast filtering; configures parameters for multicast query	401

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
IGMP Immediate Leave	Configures immediate leave for multicast services no longer required	403
Multicast Router Port Information	Displays the ports that are attached to a neighboring multicast router for each VLAN ID	405
Static Multicast Router Port Configuration	Assigns ports that are attached to a neighboring multicast router	405
IP Multicast Registration Table	Displays all multicast groups active on this switch, including multicast IP addresses and VLAN ID	406
IGMP Member Port Table	Statically assigns multicast addresses to the selected VLAN	407
IGMP Filter Configuration	Enables IGMP filtering for the switch	409
IGMP Filter Profile Configuration	Configures IGMP filter profiles, controlling groups and access mode	410
IGMP Filter/Throttling Port Configuration	Assigns IGMP filter profiles to port interfaces and sets throttling action	411
IGMP Filter/Throttling Trunk Configuration	Assigns IGMP filter profiles to trunk interfaces and sets throttling action	411
MVR	Multicast VLAN Registration	413
Configuration	Globally enables MVR, sets the MVR VLAN, adds multicast stream addresses	414
Port Information	Displays MVR interface type, MVR operational and activity status, and immediate leave status	415
Trunk Information	Displays MVR interface type, MVR operational and activity status, and immediate leave status	415
Group IP Information	Displays the ports attached to an MVR multicast stream	416
Port Configuration	Configures MVR interface type and immediate leave status	417
Trunk Configuration	Configures MVR interface type and immediate leave status	417
Group Member Configuration	Statically assigns MVR multicast streams to an interface	419
Receiver Configuration	Permits forwarding of tagged multicast traffic by specifying MVR receiver VLAN and MVR receiver groups	420
Receiver Group IP Information	Displays ports assigned to MVR receiver groups	421
Receiver Group Member Configuration	Statically assigns MVR receiver groups to selected ports	421
DNS	Domain Name Service	425
General Configuration	Enables DNS; configures domain name and domain list; and specifies IP address of name servers for dynamic lookup	425
Static Host Table	Configures static entries for domain name to address mapping	427
Cache	Displays cache entries discovered by designated name servers	428
DHCP Snooping		248
Configuration	Enables DHCP Snooping and DHCP Snooping MAC-Address Verification	250
VLAN Configuration	Enables DHCP Snooping for a VLAN	250
Information Option Configuration	Enables DHCP Snooping Information Option; and sets the information policy	251
Port Configuration	Sets the trust mode for an interface	253

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Binding Information	Displays the DHCP Snooping binding information	254
IP Source Guard	Filters IP traffic based on static entries in the IP Source Guard table, or dynamic entries in the DHCP Snooping table	255
Port Configuration	Enables IP source guard and selects filter type per port	255
Static Configuration	Adds a static addresses to the source-guard binding table	257
Dynamic Information	Displays the source-guard binding table for a selected interface	259
UPNP	Universal Plug and Play	136
Configuration	Enables UPNP and defines timeout values	137
Cluster		138
Configuration	Globally enables clustering for the switch; sets Commander status	139
Member Configuration	Adds switch Members to the cluster	140
Member Information	Displays cluster Member switch information	141
Candidate Information	Displays network Candidate switch information	141

4 BASIC MANAGEMENT TASKS

This chapter describes the following topics:

- Displaying System Information – Provides basic system description, including contact information.
- Displaying Switch Hardware/Software Versions – Shows the hardware version, power status, and firmware versions
- Displaying Bridge Extension Capabilities – Shows the bridge extension parameters.
- IP Configuration – Sets an IP address for management access.
- Configuring Support for Jumbo Frames – Enables support for jumbo frames.
- Checking System Resources – Displays information on CPU and memory utilization parameters.
- Managing System Files – Describes how to upgrade operating software or configuration files, and set the system start-up files.
- Configuring Console and Telnet Settings – Sets console port and Telnet connection parameters.
- Logging Events – Sets conditions for logging event messages to system memory or flash memory, configures conditions for sending trap messages to remote log servers, and configures trap reporting to remote hosts using Simple Mail Transfer Protocol (SMTP).
- Resetting the System – Restarts the switch immediately, at a specified time, after a specified delay, or at a periodic interval.
- Setting the System Clock – Sets the current time manually or through specified SNTP servers.
- UPnP – Configures Universal Plug-and-Play functionality on the switch.
- Switch Clustering – Configures centralized management by a single unit over a group of switches connected to the same local network

DISPLAYING SYSTEM INFORMATION

Use the System > System Information page to identify the system by displaying information such as the device name, location and contact information.

CLI REFERENCES

- "System Management Commands" on page 453
- "SNMP Commands" on page 527

PARAMETERS

These parameters are displayed in the web interface:

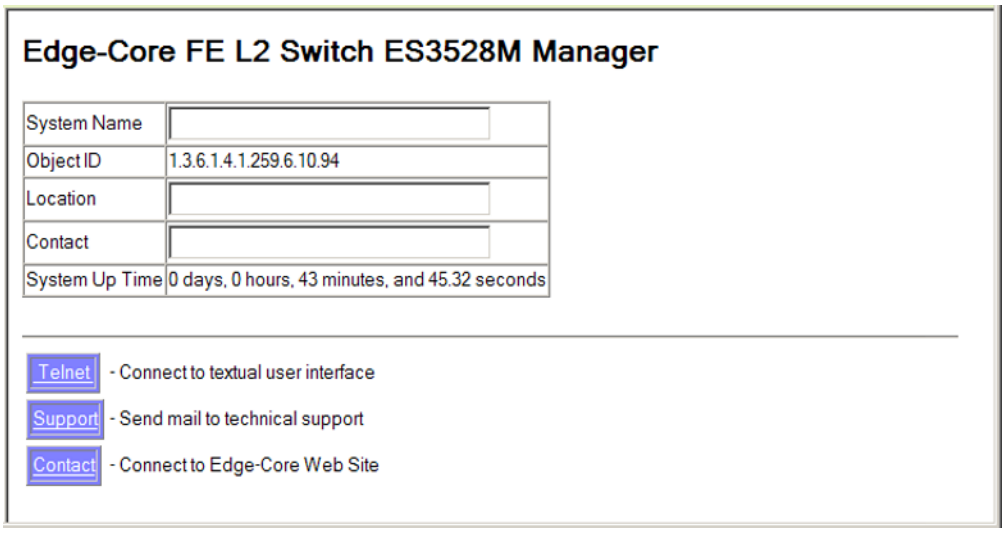
- **System Name** – Name assigned to the switch.
- **Object ID** – MIB II object ID for switch's network management subsystem.
- **Location** – Specifies the system location.
- **Contact** – Administrator responsible for the system.
- **System Up Time** – Length of time the management agent has been up.

WEB INTERFACE

To configure general system information:

1. Click System, General.
2. Specify the system name, location, and contact information for the system administrator.
3. Click Apply.

Figure 3: System Information



NOTE: This page also includes a Telnet button that allows access to the Command Line Interface via Telnet.

DISPLAYING SWITCH HARDWARE/SOFTWARE VERSIONS

Use the System > Switch Information page to display hardware/firmware version numbers for the main board and management software, as well as the power status of the system.

CLI REFERENCES

- "System Management Commands" on page 453

PARAMETERS

The following parameters are displayed in the web interface:

Main Board

- **Serial Number** – The serial number of the switch.
- **Number of Ports** – Number of built-in ports.
- **Hardware Version** – Hardware version of the main board.
- **Chip Device ID** – Identifier for basic MAC/Physical Layer switch chip.
- **Internal Power Status** – Displays the status of the internal power supply.

Management Software

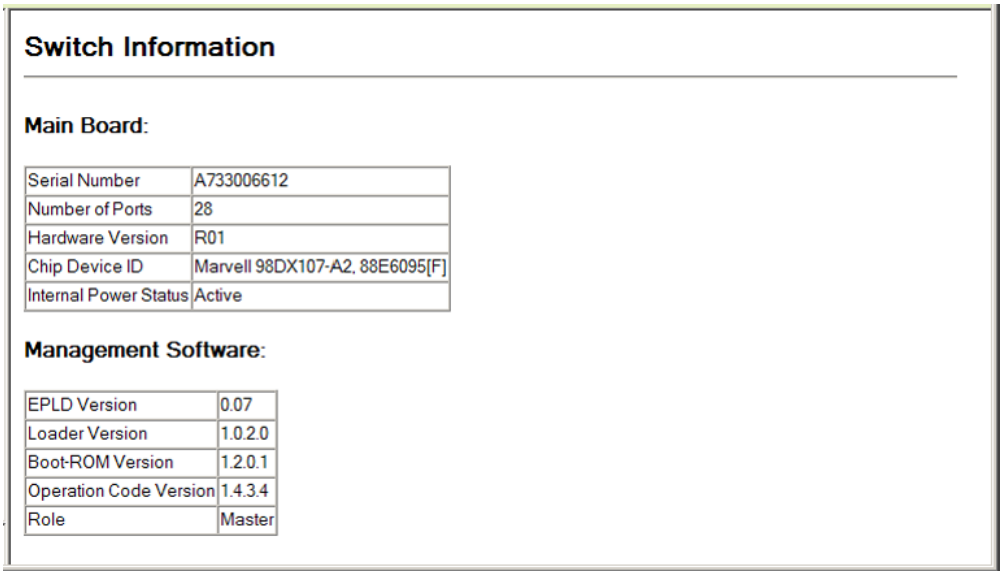
- **EPLD Version** – Version number of EEPROM Programmable Logic Device.
- **Loader Version** – Version number of loader code.
- **Boot-ROM Version** – Version of Power-On Self-Test (POST) and boot code.
- **Operation Code Version** – Version number of runtime code.
- **Role** – Shows that this switch is operating as Master or Slave.

WEB INTERFACE

To view hardware and software version information.

1. Click System, then Switch Information.

Figure 4: General Switch Information



DISPLAYING BRIDGE EXTENSION CAPABILITIES

Use the System > Bridge Extension Configuration page to display settings based on the Bridge MIB. The Bridge MIB includes extensions for managed devices that support Multicast Filtering, Traffic Classes, and Virtual LANs. You can access these extensions to display default settings for the key variables.

CLI REFERENCES

- "GVRP and Bridge Extension Commands" on page 800

PARAMETERS

The following parameters are displayed in the web interface:

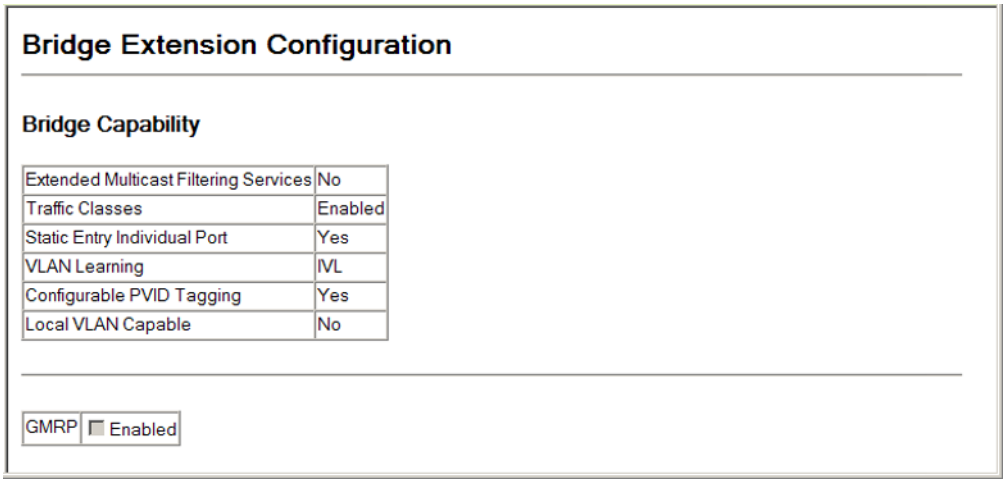
- **Extended Multicast Filtering Services** – This switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).
- **Traffic Classes** – This switch provides mapping of user priorities to multiple traffic classes. (Refer to "Class of Service" on page 375.)
- **Static Entry Individual Port** – This switch allows static filtering for unicast and multicast addresses. (Refer to "Setting Static Addresses" on page 293.)
- **VLAN Learning** – This switch uses Independent VLAN Learning (IVL), where each port maintains its own filtering database.
- **Configurable PVID Tagging** – This switch allows you to override the default Port VLAN ID (PVID used in frame tags) and egress status (VLAN-Tagged or Untagged) on each port. (Refer to "VLAN Configuration" on page 327.)
- **Local VLAN Capable** – This switch does not support multiple local bridges outside of the scope of 802.1Q defined VLANs.
- **GMRP** – GARP Multicast Registration Protocol (GMRP) allows network devices to register end stations with multicast groups. This switch does not support GMRP; it uses the Internet Group Management Protocol (IGMP) to provide automatic multicast filtering.

WEB INTERFACE

To view Bridge Extension information:

1. Click System, then Bridge Extension Configuration.

Figure 5: Displaying Bridge Extension Configuration



SETTING THE SWITCH'S IP ADDRESS

Use the System > IP Configuration page to configure an IP address for management access over the network. An IP address is obtained via DHCP by default for VLAN 1. To configure a static address, you need to change the switch's default settings to values that are compatible with your network. You may also need to a establish a default gateway between the switch and management stations that exist on another network segment.

You can direct the device to obtain an address from a BOOTP or DHCP server, or manually configure a static IP address. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything other than this format will not be accepted.

CLI REFERENCES

- "DHCP Client" on page 935
- "IP Interface Commands" on page 943

PARAMETERS

These parameters are displayed:

- **Management VLAN** – ID of the configured VLAN (1-4094). By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address.

- **IP Address Mode** – Specifies whether IP functionality is enabled via manual configuration (Static), Dynamic Host Configuration Protocol (DHCP), or Boot Protocol (BOOTP). If DHCP/BOOTP is enabled, IP will

not function until a reply has been received from the server. Requests will be broadcast periodically by the switch for an IP address. DHCP/ BOOTP responses can include the IP address, subnet mask, and default gateway. (Default: Static)

- **IP Address** – Address of the VLAN to which the management station is attached. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: 0.0.0.0)
- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets. (Default: 255.0.0.00)
- **Gateway IP Address** – IP address of the gateway router between the switch and management stations that exist on other network segments. (Default: 0.0.0.0)
- **MAC Address** – The physical layer address for this switch.
- **DHCP Relay Option 82** – Enables relay agent information option for sending information about its DHCP clients to the DHCP server.

  DHCP provides a relay agent information option for sending information about its DHCP clients to the DHCP server. Also known as DHCP Option 82, it allows compatible DHCP servers to use this information when assigning IP addresses, or to set other services or policies for clients.

  When Option 82 is enabled, the requesting client (or an intermediate relay agent that has used the information fields to describe itself) can be identified in the DHCP request packets forwarded by the switch and in reply packets sent back from the DHCP server. Depending on the selected frame format for the remote-id set by the ip dhcp relay information option command, this information may specify the MAC address or IP address of the requesting device (that is, the relay agent in this context).

  By default, the relay agent also fills in the Option 82 circuit-id field with information indicating the local interface over which the switch received the DHCP client request, including the stack unit, port, and VLAN ID.

  If Option 82 is enabled on the switch, client information will be included in any relayed request packet received over any VLAN according to this criteria.

Table 7: Inserting Option 82 Information - display description

DHCP Relay*	DHCP Option 82	Action
Disabled	Enabled	Circuit-id and remote-id are added to the Option 82 packet, but the gateway Internet address is not included.
Enabled	Enabled	Circuit-id and remote-id are added to the option 82 packet, and the gateway Internet address is included.

* DHCP Relay is enabled if a DHCP relay server is specified.

- DHCP request packets are flooded onto the VLAN which received the request if DHCP relay service is enabled on the switch, and the request packet contains a valid (i.e., non-zero) relay agent address field.

- DHCP reply packets received by the relay agent are handled as follows:

  1. When the relay agent receives a DHCP reply packet with Option 82 information on the management VLAN, it first ensures that the packet is destined for it, and then removes the Option 82 field from the packet.

  2. If the DHCP packet's broadcast flag is on, the switch uses the circuit-id information contained in the option 82 information fields to identify the VLAN connected to the requesting client and then broadcasts the DHCP reply packet to this VLAN. If the DHCP packet's broadcast flag is off, the switch uses the circuit-id information in option 82 fields to identify the interface connected to the requesting client and unicasts the reply packet to the client

- DHCP reply packets are flooded onto the VLAN which received the reply if DHCP relay service is enabled and any of the following situations apply:

  - The reply packet does not contain Option 82 information.

  - The reply packet contains a valid relay agent address field (that is not the address of this switch), or receives a reply packet with a zero relay agent address through the management VLAN.

  - The reply packet is received on a non-management VLAN.

- **DHCP Relay Option 82 Policy** – Specifies how to handle DHCP client request packets which already contain Option 82 information:

  - **Drop** – Floods the request packet onto the VLAN that received the original request instead of relaying it.

  - **Keep** – Retains the Option 82 information in the client request, inserts the relay agent's address, and unicasts the packet to the DHCP server.

  - When the Option 82 policy is set to "keep" the original information in the request packet, the frame type specified by the ip dhcp relay information option command is ignored.

  - **Replace** – Replaces the Option 82 information circuit-id and remote-id fields in the client's request with information provided by the relay agent itself, inserts the relay agent's address, and unicasts the packet to the DHCP server. (This is the default policy.)

- **DHCP Relay Server** – Specifies the DHCP servers to be used by the switch's DHCP relay agent in order of preference.

  This switch supports DHCP relay service for attached host devices. If DHCP relay is enabled (by specifying the address for at least one DHCP server), and this switch sees a DHCP request broadcast, it inserts its own IP address into the request so that the DHCP server will know the subnet where the client is located. Then, the switch forwards the packet to the DHCP server. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client's subnet, and sends a DHCP response back to the DHCP relay agent (i.e., this switch). This switch then passes the DHCP response received from the server to the client.

  You must specify the IP address for at least one DHCP server. Otherwise, the switch's DHCP relay agent will not forward client requests to a DHCP server.

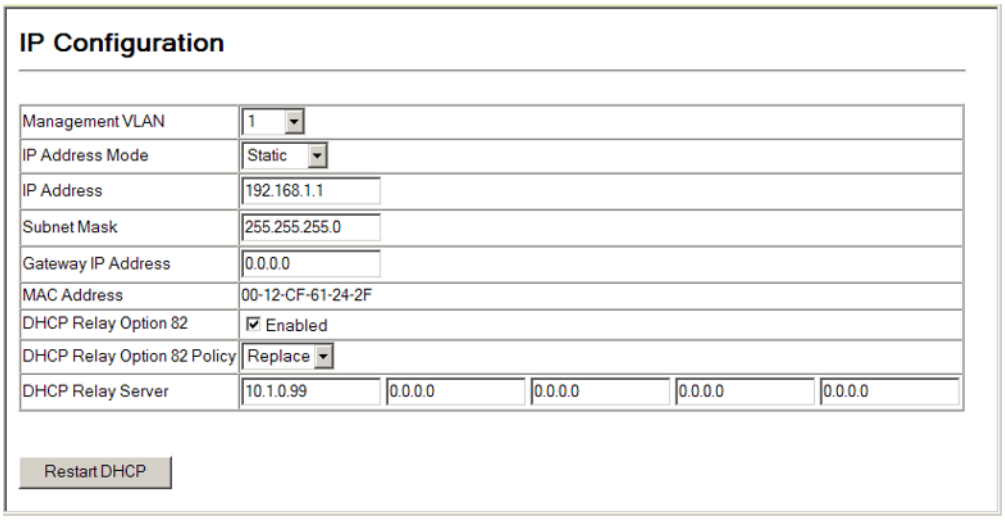
- **Restart DHCP** – Requests a new IP address from the DHCP server.

WEB INTERFACE

To set a static address for the switch:

1. Click System, IP Configuration.
2. Select the VLAN through which the management station is attached, set the IP Address Mode to "Static," enter the IP address, subnet mask and gateway. Specify the required settings for DHCP Relay Option. Enter the DHCP Relay Servers to use in order of preference.
3. Click Apply.

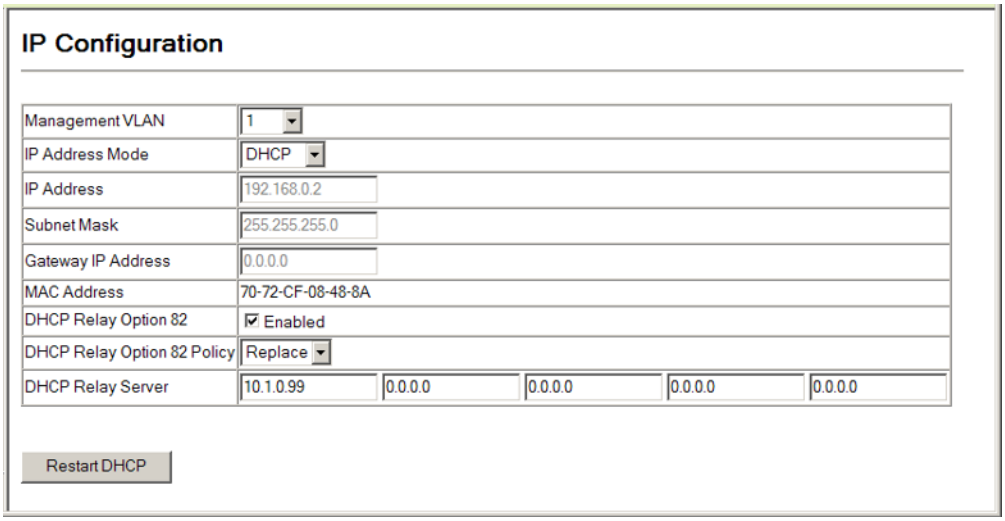
Figure 6: Configuring a Static IP Address



To obtain an dynamic address through DHCP/BOOTP for the switch:

1. Click System, IP Configuration.
2. Select the VLAN through which the management station is attached, set the IP Address Mode to "DHCP" or "BOOTP."
3. Click Apply to save your changes.
4. Then click Restart DHCP to immediately request a new address.

Figure 7: Configuring a Dynamic IPv4 Address



NOTE: The switch will also broadcast a request for IP configuration settings on each power reset.

NOTE: If you lose the management connection, make a console connection to the switch and enter "show ip interface" to determine the new switch address.

Renewing DCHP – DHCP may lease addresses to clients indefinitely or for a specific period of time. If the address expires or the switch is moved to another network segment, you will lose management access to the switch. In this case, you can reboot the switch or submit a client request to restart DHCP service via the CLI.

If the address assigned by DHCP is no longer functioning, you will not be able to renew the IP settings via the web interface. You can only restart DHCP service via the web interface if the current address is still available.

CONFIGURING SUPPORT FOR JUMBO FRAMES

Use the System > Jumbo Frames page to configure support for jumbo frames. The switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames up to 10 KB for the Gigabit Ethernet ports. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

CLI REFERENCES

- "System Management Commands" on page 453

USAGE GUIDELINES

To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.

PARAMETERS

The following parameters are displayed in the web interface:

- **Jumbo Packet Status** – Configures support for jumbo frames. (Default: Disabled)

WEB INTERFACE

To configure support for jumbo frames:

1. Click System, then Jumbo Frames.
2. Enable or disable support for jumbo frames.
3. Click Apply.

Figure 8: Configuring Support for Jumbo Frames

DISPLAYING CPU UTILIZATION

Use the System > Resource > CPU Status page to display information on CPU utilization; or to set thresholds for the CPU utilization alarm.

CLI REFERENCES

- "show process cpu" on page 464

PARAMETERS

The following parameters are displayed in the web interface:

- **Current CPU Utilization** – CPU utilization over the past 5 seconds.
- **Maximum CPU Utilization** – Peak CPU utilization over past 60 seconds.
- **Average CPU Utilization** – Average CPU utilization over past 60 seconds.
- **CPU Peak Time** – Time when CPU reached peak utilization since last reset.
- **CPU Peak Duration** – Duration CPU ran at peak utilization since system boot.
- **CPU Utilization Rising Threshold**[1] – Rising threshold for CPU utilization alarm. (Range: 1-100%; Default: 90%)
- **CPU Utilization Falling Threshold**[1] – Falling threshold for CPU utilization alarm. (Range: 1-100%; Default: 70%)

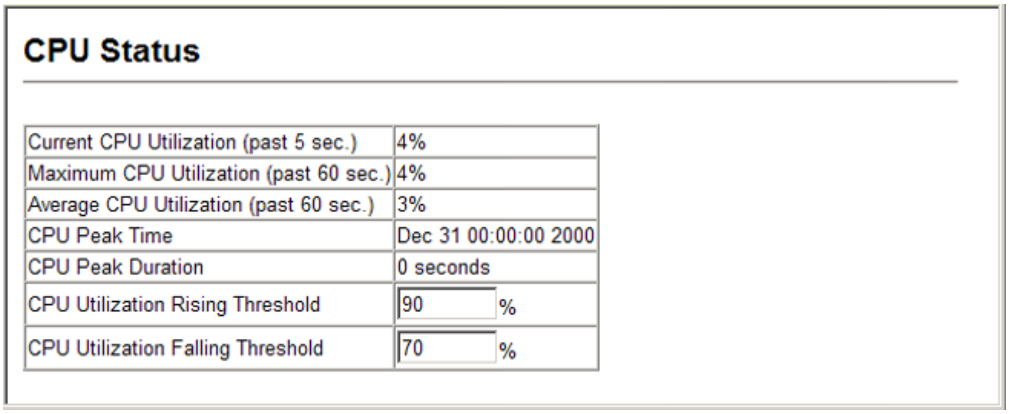
WEB INTERFACE

To display CPU utilization:

1. Click System, Resource, then CPU Status.
2. Modify threshold values for the CPU utilization alarm if required.
3. Click Apply.

1. Once the rising alarm threshold is exceeded, utilization must drop beneath the falling threshold before the alarm is terminated, and then exceed the rising threshold again before another alarm is triggered.

Figure 9: Displaying CPU Utilization



DISPLAYING MEMORY UTILIZATION

Use the System > Resource > Memory Status page to display memory utilization parameters; or to set thresholds for the memory utilization alarm.

CLI REFERENCES

- "show memory" on page 464

PARAMETERS

The following parameters are displayed in the web interface:

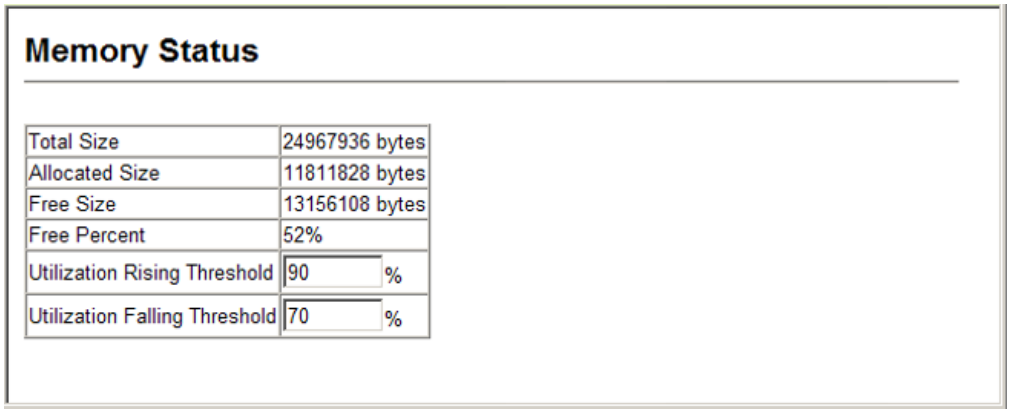
- **Total Size** – Total amount of memory provided by the system.
- **Allocated Size** – Amount of memory allocated to active processes.
- **Free Size** – Amount of memory currently free for use.
- **Free Percent** – Percentage of free memory compared to total memory.
- **Utilization Raising Threshold**[1] – Rising threshold for memory utilization alarm. (Range: 1-100%; Default: 90%)
- **Utilization Falling Threshold**[1] – Falling threshold for memory utilization alarm. (Range: 1-100%; Default: 90%)

WEB INTERFACE

To display memory utilization:

1. Click System, Resource, then Memory Status.
2. Modify threshold values for the memory utilization alarm if required.
3. Click Apply.

Figure 10: Displaying Memory Utilization



MANAGING SYSTEM FILES

This section describes how to upgrade the switch operating software or configuration files, and set the system start-up files.

AUTOMATIC OPERATION CODE UPGRADE

The system can be configured to automatically download an operation code file when a file newer than the currently installed one is discovered on the file server. After the file is transferred from the server and successfully written to the file system, it is automatically set as the startup file, and the switch is rebooted.

CLI REFERENCES

- "upgrade opcode auto" on page 478
- "upgrade opcode path" on page 480
- "show upgrade" on page 481

COMMAND USAGE

- If this feature is enabled, the switch searches the defined URL once during the bootup sequence.
- FTP (port 21) and TFTP (port 69) are both supported. Note that the TCP/UDP port bindings cannot be modified to support servers listening on non-standard ports.
- The host portion of the upgrade file location URL must be a valid IPv4 IP address. DNS host names are not recognized. Valid IP addresses consist of four numbers, 0 to 255, separated by periods.
- The path to the directory must also be defined. If the file is stored in the root directory for the FTP/TFTP service, then use the "/" to indicate this (e.g., ftp://192.168.0.1/).
- The file name must not be included in the upgrade file location URL. The file name of the code stored on the remote server must be

ES3552M-PoE.bix (using upper case and lower case letters exactly as indicated here).

- The FTP connection is made with PASV mode enabled. PASV mode is needed to traverse some fire walls, even if FTP traffic is not blocked. PASV mode cannot be disabled.

- The switch-based search function is case-insensitive in that it will accept a file name in upper or lower case (i.e., the switch will accept *ES3552M-PoE.BIX* from the server even though *es3552m-poe.bix* was requested). However, keep in mind that the file systems of many operating systems such as Unix and most Unix-like systems (FreeBSD, NetBSD, OpenBSD, and most Linux distributions, etc.) are case-sensitive, meaning that two files in the same directory, *es3552m-poe.bix* and *ES3552M-PoE.BIX* are considered to be unique files. Thus, if the upgrade file is stored as *ES3552M-PoE.BIX* (or even *Es3552m-poe.bix*) on a case-sensitive server, then the switch (requesting *es3552m-poe.bix*) will not be upgraded because the server does not recognize the requested file name and the stored file name as being equal. A notable exception in the list of case-sensitive Unix-like operating systems is Mac OS X, which by default is case-insensitive. Please check the documentation for your server's operating system if you are unsure of its file system's behavior.

  Note that the switch itself does not distinguish between upper and lower-case file names, and only checks to see if the file stored on the server is more recent than the current runtime image.

- If two operation code image files are already stored on the switch's file system, then the non-startup image is deleted before the upgrade image is transferred.

- The automatic upgrade process will take place in the background without impeding normal operations (data switching, etc.) of the switch.

- During the automatic search and transfer process, the administrator cannot transfer or update another operation code image, configuration file, public key, or HTTPS certificate (i.e., no other concurrent file management operations are possible).

- The upgrade operation code image is set as the startup image after it has been successfully written to the file system.

- The switch will send an SNMP trap and make a log entry upon all upgrade successes and failures.

- The switch will immediately restart after the upgrade file is successfully written to the file system and set as the startup image.

PARAMETERS

The following parameters are displayed in the web interface:

- **Automatic Opcode Upgrade** – Enables the switch to search for an upgraded operation code file during the switch bootup process.
  - **Enabled** *check box* – Defines the state of this feature. (Default: Disabled)
- **Automatic Upgrade Location URL** – Defines where the switch should search for the operation code upgrade file. The last character of this URL must be a forward slash ("/"). The *ES3552M-PoE.bix* filename must not be included since it is automatically appended by the switch. (Options: ftp, tftp)

  The following syntax must be observed:

  tftp://*host*[/*filedir*]/

  tftp:// – Defines TFTP protocol for the server connection.
  host – Defines the IP address of the TFTP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. DNS host names are not recognized.
  filedir – Defines the directory, relative to the TFTP server root, where the upgrade file can be found. Nested directory structures are accepted. The directory name must be separated from the host, and in nested directory structures, from the parent directory, with a prepended forward slash "/".
  / – The forward slash must be the last character of the URL.

  ftp://[***username***[**:*password*@**]]***host***[/***filedir***]**/**

  ftp:// – Defines FTP protocol for the server connection.
  username – Defines the user name for the FTP connection. If the user name is omitted, then "anonymous" is the assumed user name for the connection.
  password – Defines the password for the FTP connection. To differentiate the password from the user name and host portions of the URL, a colon (:) must precede the password, and an "at" symbol (@), must follow the password. If the password is omitted, then "" (an empty string) is the assumed password for the connection.
  host – Defines the IP address of the FTP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. DNS host names are not recognized.
  filedir – Defines the directory, relative to the FTP server root, where the upgrade file can be found. Nested directory structures are accepted. The directory name must be separated from the host, and in nested directory structures, from the parent directory, with a prepended forward slash "/".
  / – The forward slash must be the last character of the URL.
- **File Name** – The name of the operation code file on the file TFTP or FTP server. Remember that this name should not be included in the

upgrade path of the preceding item since it is automatically appended by the switch.

EXAMPLES

- The following examples demonstrate the URL syntax for a TFTP server at IP address 192.168.0.1 with the operation code image stored in various locations:

  - **tftp://192.168.0.1/**
    The image file is in the TFTP root directory.

  - **tftp://192.168.0.1/switch-opcode/**
    The image file is in the "switch-opcode" directory, relative to the TFTP root.

  - **tftp://192.168.0.1/switches/opcode/**
    The image file is in the "opcode" directory, which is within the "switches" parent directory, relative to the TFTP root.

- The following examples demonstrate the URL syntax for an FTP server at IP address 192.168.0.1 with various user name, password and file location options presented:

  - ftp://192.168.0.1/
    The user name and password are empty, so "anonymous" will be the user name and the password will be blank. The image file is in the FTP root directory.

  - ftp://switches:upgrade@192.168.0.1/
    The user name is "switches" and the password is "upgrade". The image file is in the FTP root.

  - **ftp://switches:upgrade@192.168.0.1/switches/opcode/**
    The user name is "switches" and the password is "upgrade". The image file is in the "opcode" directory, which is within the "switches" parent directory, relative to the FTP root.

WEB INTERFACE

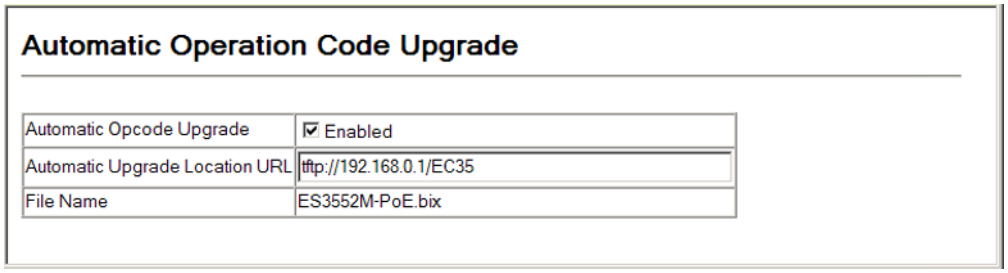
To automatically download an operation code file from a file server:

1. Click System, File Management, then Automatic Operation Code Upgrade.

2. Check the Automatic Opcode Upgrade box, enter the URL of the FTP or TFTP server, the path and directory containing the operation code.

3. Click Apply.

Figure 11: Configuring Automatic Code Upgrade



If a new image is found at the specified location, the following type of messages will be displayed on the console interface during bootup.

```
⋮
Automatic Upgrade is looking for a new image
New image detected: current version 1.1.1.0; new version 1.1.1.2
Image upgrade in progress
The switch will restart after upgrade succeeds
Downloading new image
Flash programming started
Flash programming completed
The switch will now restart
⋮
```

COPYING OPERATION CODE VIA FTP OR TFTP

Use the System > File (Copy) page to upload/download firmware or configuration settings using FTP or TFTP. By backing up a file to an FTP or TFTP server or management station, that file can later be downloaded to the switch to restore operation. Specify the method of file transfer, along with the file type and file names as required.

You can also set the switch to use new firmware or configuration settings without overwriting the current version. Just download the file using a different name from the current version, and then set the new file as the startup file.

NOTE: You can also download and upload files to the switch using HTTP, see "Copying Files Using HTTP" on page 116.

CLI REFERENCES

- "copy" on page 473
- "dir" on page 477

PARAMETERS

The following parameters are displayed in the web interface:

- **File Transfer Method** – The firmware copy operation includes these options:
  - file to file – Copies a file within the switch directory, assigning it a new name.

- file to ftp – Copies a file from the switch to an FTP server.
- file to tftp – Copies a file from the switch to a TFTP server.
- ftp to file – Copies a file from an FTP server to the switch.
- tftp to file – Copies a file from a TFTP server to the switch.

- **FTP/TFTP Server IP Address** – IP address of an FTP or TFTP server.
- **User Name** – The user name for FTP server access.
- **Password** – The password for FTP server access.
- **File Type** – Specify opcode (operation code) to copy firmware.
- **File Name** – The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names is 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

NOTE: Up to two copies of the system software (i.e., the runtime firmware) can be stored in the file directory on the switch.

NOTE: The maximum number of user-defined configuration files is limited only by available flash memory space.

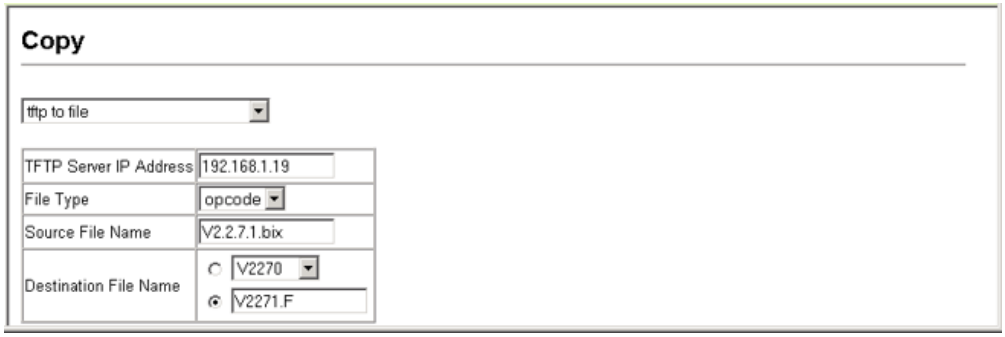
NOTE: The file "Factory_Default_Config.cfg" can be copied to a file server or management station, but cannot be used as the destination file name on the switch.

WEB INTERFACE

To copy firmware files:

1. Click System, File Management, then Copy Operation.
2. Select "tftp to file" or "ftp to file" as the file transfer method.
3. If FTP or TFTP Upgrade is used, enter the IP address of the file server.
4. If FTP Upgrade is used, enter the user name and password for your account on the FTP server.
5. Set the file type to opcode.
6. Enter the name of the file to download.
7. Select a file on the switch to overwrite or specify a new file name.
8. Then click Apply.

Figure 12: Copying Firmware



If you download to a new destination file, go to the System > File Management > Set Start-Up menu, mark the operation code file used at startup, and click Apply. To start the new firmware, reboot the system via the System > Reset menu.

If you replaced a file currently used for startup and want to start using the new file, reboot the system via the System > Reset menu.

SAVING OR RESTORING CONFIGURATION SETTINGS

Use the System > File Management > Copy Operation page to upload/download configuration settings to/from an FTP/TFTP server. The configuration settings are not automatically saved by the system for subsequent use when the switch is rebooted. You must save these settings to the current startup file, or to another file which can be subsequently set as the startup file. If you copy the configuration settings to a file server, this information can be later downloaded to restore the switch's settings.

CLI REFERENCES

- "copy" on page 473

PARAMETERS

The following parameters are displayed in the web interface:

- **File Transfer Method** – The configuration copy operation includes these options:
  - file to file – Copies a file within the switch directory, assigning it a new name.
  - file to ftp – Copies a file from the switch to an FTP server.
  - file to running-config – Copies a file in the switch to the running configuration.
  - file to startup-config – Copies a file in the switch to the startup configuration.
  - file to tftp – Copies a file from the switch to a TFTP server.
  - ftp to file – Copies a file from an FTP server to the switch.
  - tftp to file – Copies a file from a TFTP server to the switch.
  - ftp to running-config – Copies a file from an FTP server to the running config.

- ftp to startup-config – Copies a file from an FTP server to the startup config.
- running-config to file – Copies the running configuration to a file.
- running-config to ftp – Copies the running configuration to an FTP server.
- running-config to startup-config – Copies the running config to the startup config.
- running-config to tftp – Copies the running configuration to a TFTP server.
- startup-config to file – Copies the startup configuration to a file on the switch.
- startup-config to ftp – Copies the startup configuration to an FTP server.
- startup-config to running-config – Copies the startup config to the running config.
- startup-config to tftp – Copies the startup configuration to a TFTP server.
- tftp to file – Copies a file from a TFTP server to the switch.
- tftp to running-config – Copies a file from a TFTP server to the running config.
- tftp to startup-config – Copies a file from a TFTP server to the startup config.

- **FTP/TFTP Server IP Address** – The IP address of an FTP or TFTP server.

  The server's location must be specified as a valid IPv4 IP address. DNS host names are not recognized. Valid IP addresses consist of four numbers, 0 to 255, separated by periods.

  FTP (port 21) and TFTP (port 69) are both supported.

- **User Name** – The user name for FTP server access.

- **Password** – The password for FTP server access.

- **File Type** – Specify config (configuration) to copy configuration settings.

- **File Name** – The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names is 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

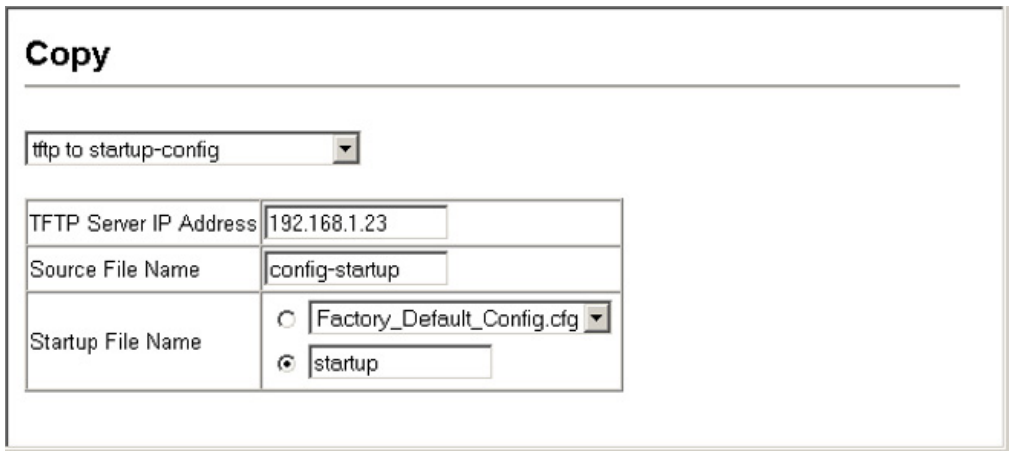
NOTE: The maximum number of user-defined configuration files is limited only by available flash memory space.

WEB INTERFACE

To save the running configuration file:

1. Click System, File Management > Copy Operation.
2. Select "tftp to startup-config" or "tftp to file" and enter the IP address of the TFTP server. If you download from an FTP server, enter the user name and password for an account on the server. Specify the name of the file to download and select a file on the switch to overwrite or specify a new file name.
3. Then click Apply.

Figure 13: Copying Configuration Settings



If you replaced a file currently used for startup and want to start using the new file, reboot the system via the System > Reset menu.

COPYING FILES USING HTTP

In addition to performing copy operations to and from an FTP or TFTP server, the switch can upload or download files to the web management station using HTTP.

Both switch operation code files and configuration files can be uploaded/ downloaded using HTTP.

PARAMETERS

The following parameters are displayed in the web interface:

- **File Type** – Specify opcode (operation code) to copy a firmware file, or config (configuration) to copy a switch configuration file.
- **Source File Name** – Use the Browse button to locate the file on the web management station. The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on is 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

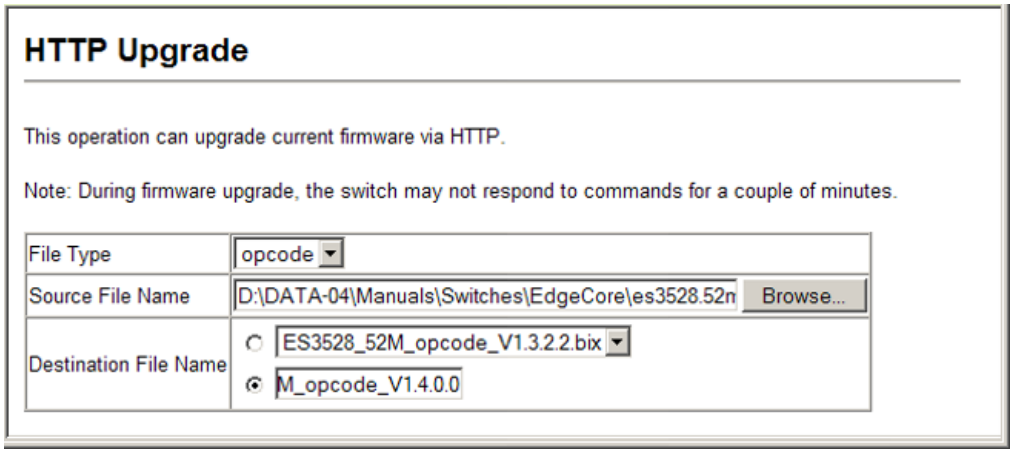
- **Destination File Name** – Select an existing file on the switch to overwrite, or specify a new file name.

WEB INTERFACE

To upload files to the switch from your management station using HTTP:

1. Click System, File Management > HTTP Upgrade.
2. Select "opcode" or "config" as the file type and then use the Browse button to locate the file on the local web management station. Specify the name of a file on the switch to overwrite or specify a new file name.
3. Then click Apply.

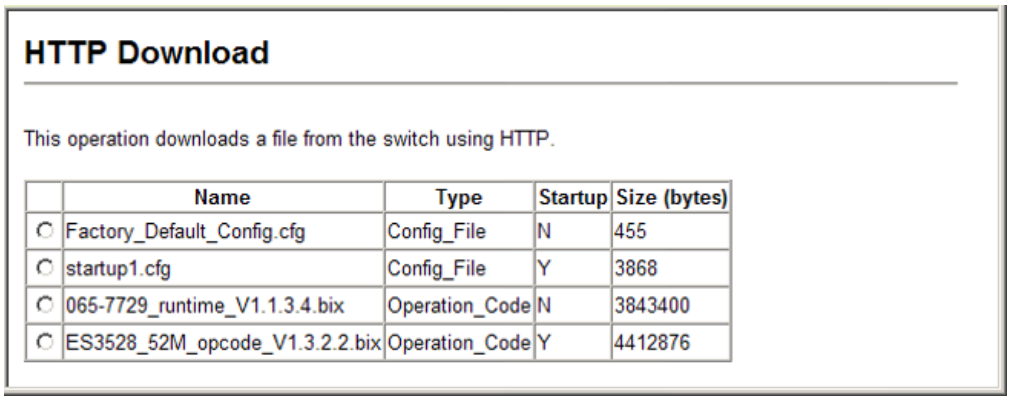
Figure 14: Uploading Files Using HTTP



To download files to your management station from the switch using HTTP:

1. Click System, File Management > HTTP Download.
2. Select an operation code file or configuration file on the switch to download to the web management station.
3. Then click Apply.

Figure 15: Downloading Files Using HTTP



DELETING FILES

Use the System > File Management > Delete page to delete a file from the switch.

CLI REFERENCES

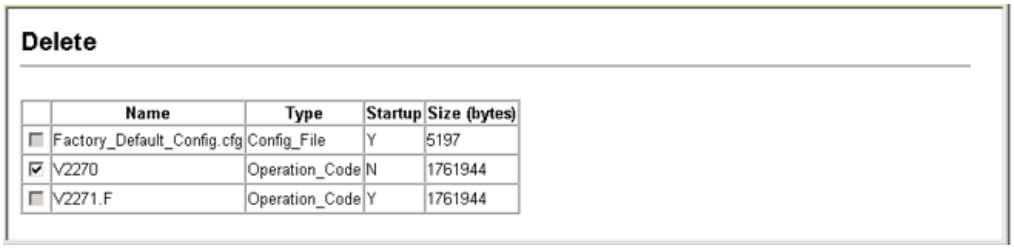
- "delete" on page 476
- "delete non-active" on page 476

WEB INTERFACE

To delete a file from the switch:

1. Click System, File Management, then Delete.
2. Mark the file to be deleted
3. Then click Apply.

Figure 16: Deleting Files



SETTING THE START-UP FILE

Use the System > File Management > Set Start-Up page to specify the firmware or configuration file to use for system initialization.

CLI REFERENCES

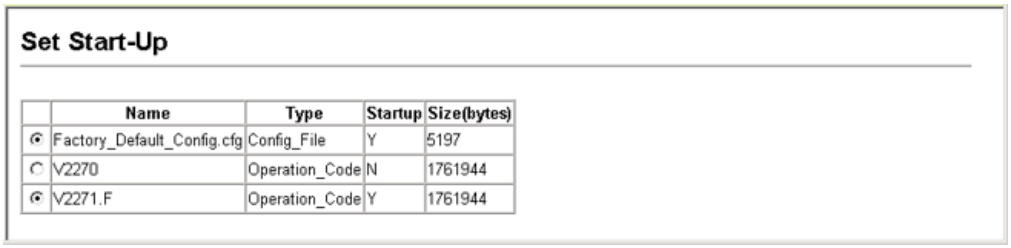
- "whichboot" on page 478
- "boot system" on page 472

WEB INTERFACE

To set a file to use for system initialization:

1. Click System, File Management, then Set Start-Up.
2. Mark the operation code or configuration file to be used at startup
3. Then click Apply.

Figure 17: Setting the Start-up Code



To start using the new firmware or configuration settings, reboot the system via the System > Reset menu.

CONSOLE PORT SETTINGS

Use the System > Line > Console menu to configure connection parameters for the switch's console port. You can access the onboard configuration program by attaching a VT100 compatible device to the switch's serial console port. Management access through the console port is controlled by various parameters, including a password (only configurable through the CLI), time outs, and basic communication settings. Note that these parameters can be configured via the web or CLI interface.

CLI REFERENCES

- "Line" on page 481

PARAMETERS

The following parameters are displayed in the web interface:

- **Login Timeout** – Sets the interval that the system waits for a user to log into the CLI. If a login attempt is not detected within the timeout interval, the connection is terminated for the session. (Range: 0-300 seconds; Default: 0 seconds)
- **Exec Timeout** – Sets the interval that the system waits until user input is detected. If user input is not detected within the timeout interval, the current session is terminated. (Range: 0-65535 seconds; Default: 600 seconds)
- **Password Threshold** – Sets the password intrusion threshold, which limits the number of failed logon attempts. When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time (set by the Silent Time parameter) before allowing the next logon attempt. (Range: 0-120; Default: 3 attempts)
- **Silent Time** – Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts has been exceeded. (Range: 0-65535 seconds; Default: Disabled)
- **Data Bits** – Sets the number of data bits per character that are interpreted and generated by the console port. If parity is being

generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character. (Default: 8 bits)

- **Parity** – Defines the generation of a parity bit. Communication protocols provided by some terminals can require a specific parity bit setting. Specify Even, Odd, or None. (Default: None)
- **Speed** – Sets the terminal line's baud rate for transmit (to terminal) and receive (from terminal). Set the speed to match the baud rate of the device connected to the serial port. (Range: 9600, 19200, or 38400 baud; Default: 9600 baud)
- **Stop Bits** – Sets the number of the stop bits transmitted per byte. (Range: 1-2; Default: 1 stop bit)

NOTE: The password for the console connection can only be configured through the CLI (see the password command).

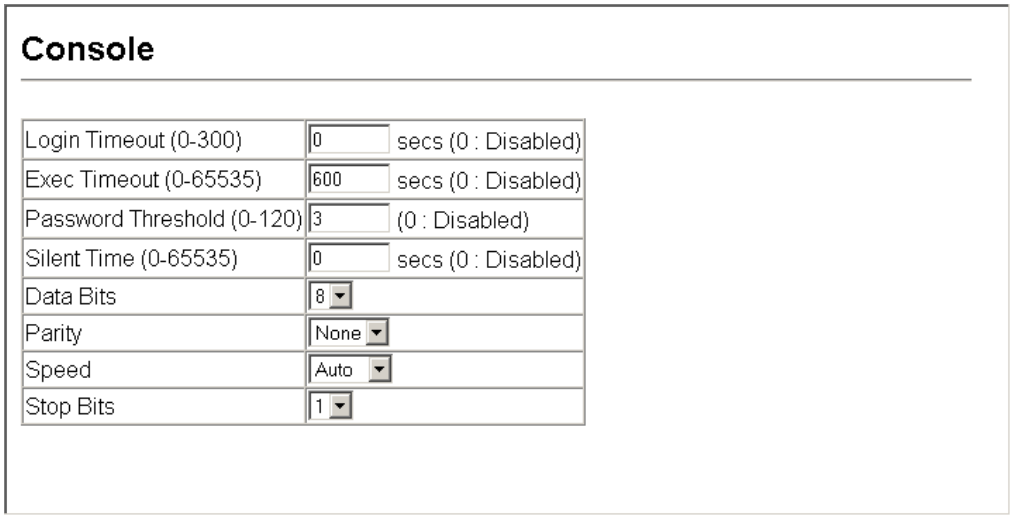
NOTE: Password checking can be enabled or disabled for logging in to the console connection (see the login command). You can select authentication by a single global password as configured for the password command, or by passwords set up for specific user-name accounts. The default is for local passwords configured on the switch.

WEB INTERFACE

To configure parameters for the console port:

1. Click System, Line, then Console.
2. Specify the connection parameters as required.
3. Click Apply

Figure 18: Console Port Settings



TELNET SETTINGS

Use the System > Line > Telnet menu to configure parameters for accessing the CLI over a Telnet connection. You can access the onboard configuration program over the network using Telnet (i.e., a virtual terminal). Management access via Telnet can be enabled/disabled and other parameters set, including the TCP port number, time outs, and a password. Note that the password is only configurable through the CLI.) These parameters can be configured via the web or CLI interface.

CLI REFERENCES

- "Line" on page 481

PARAMETERS

The following parameters are displayed in the web interface:

- **Telnet Status** – Enables or disables Telnet access to the switch. (Default: Enabled)
- **Telnet Port Number** – Sets the TCP port number for Telnet on the switch. (Default: 23)
- **Login Timeout** – Sets the interval that the system waits for a user to log into the CLI. If a login attempt is not detected within the timeout interval, the connection is terminated for the session. (Range: 0-300 seconds; Default: 300 seconds)
- **Exec Timeout** – Sets the interval that the system waits until user input is detected. If user input is not detected within the timeout interval, the current session is terminated. (Range: 0-65535 seconds; Default: 600 seconds)
- **Password Threshold** – Sets the password intrusion threshold, which limits the number of failed logon attempts. When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time (set by the Silent Time parameter) before allowing the next logon attempt. (Range: 0-120; Default: 3 attempts)

NOTE: The password for the Telnet connection can only be configured through the CLI (see the password command).

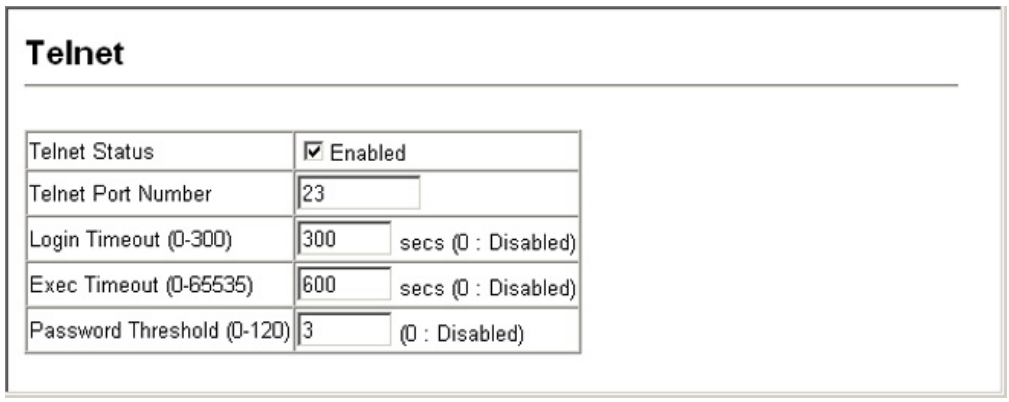
NOTE: Password checking can be enabled or disabled for login to the console connection (see the login command). You can select authentication by a single global password as configured for the password command, or by passwords set up for specific user-name accounts. The default is for local passwords configured on the switch.

WEB INTERFACE

To configure parameters for the console port:

1. Click System, Line, then Telnet.
2. Specify the connection parameters as required.
3. Click Apply

Figure 19: Telnet Connection Settings



CONFIGURING EVENT LOGGING

The switch allows you to control the logging of error messages, including the type of events that are recorded in switch memory, logging to a remote System Log (syslog) server, and displays a list of recent event messages.

SYSTEM LOG CONFIGURATION

Use the System > Log > System Logs page to enable or disable event logging, and specify which levels are logged to RAM or flash memory.

Severe error messages that are logged to flash memory are permanently stored in the switch to assist in troubleshooting network problems. Up to 4096 log entries can be stored in the flash memory, with the oldest entries being overwritten first when the available log memory (256 kilobytes) has been exceeded.

The System Logs page allows you to configure and limit system messages that are logged to flash or RAM memory. The default is for event levels 0 to 3 to be logged to flash and levels 0 to 7 to be logged to RAM.

CLI REFERENCES

- "Event Logging" on page 491

PARAMETERS

These parameters are displayed:

- **System Log Status** – Enables/disables the logging of debug or error messages to the logging process. (Default: Enabled)
- **Flash Level** – Limits log messages saved to the switch's permanent flash memory for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be logged to flash. (Range: 0-7, Default: 3)

Table 8: Logging Levels

Level	Severity Name	Description
7	Debug	Debugging messages
6	Informational	Informational messages only
5	Notice	Normal but significant condition, such as cold start
4	Warning	Warning conditions (e.g., return false, unexpected return)
3	Error	Error conditions (e.g., invalid input, default used)
2	Critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
1	Alert	Immediate action needed
0	Emergency	System unusable

* There are only Level 2, 5 and 6 error messages for the current firmware release.

- **RAM Level** – Limits log messages saved to the switch's temporary RAM memory for all levels up to the specified level. For example, if level 7 is specified, all messages from level 0 to level 7 will be logged to RAM. (Range: 0-7, Default: 7)

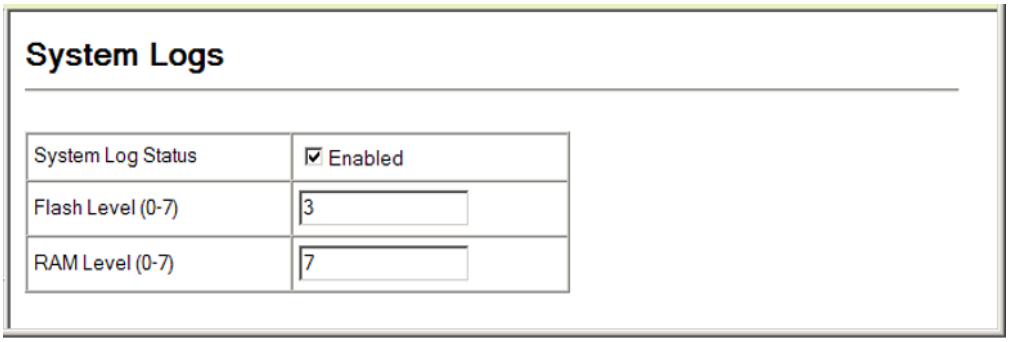
NOTE: The Flash Level must be equal to or less than the RAM Level.

WEB INTERFACE

To configure the logging of error messages to system memory:

1. Click System, Log, System Logs.
2. Enable or disable system logging, set the level of event messages to be logged to flash memory and RAM.
3. Click Apply.

Figure 20: Configuring Settings for System Memory Logs

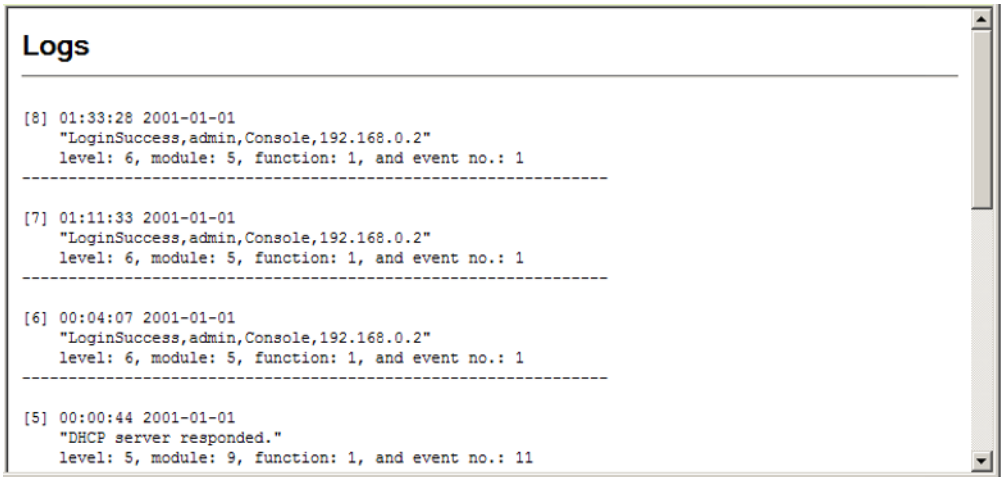


To show the error messages logged to system memory:

1. Click System, Log, Logs.

   This page allows you to scroll through the logged system and event messages. The switch can store up to 2048 log entries in temporary random access memory (RAM; i.e., memory flushed on power reset) and up to 4096 entries in permanent flash memory.

Figure 21: Showing Error Messages Logged to System Memory



REMOTE LOG CONFIGURATION

Use the System > Log > Remote Logs page to send log messages to syslog servers or other management stations. You can also limit the event messages sent to only those messages below a specified level.

CLI REFERENCES

- "Event Logging" on page 491

PARAMETERS

These parameters are displayed:

- **Remote Log Status** – Enables/disables the logging of debug or error messages to the remote logging process. (Default: Disabled)

- **Logging Facility** – Sets the facility type for remote logging of syslog messages. There are eight facility types specified by values of 16 to 23. The facility type is used by the syslog server to dispatch log messages to an appropriate service.

  The attribute specifies the facility type tag sent in syslog messages (see RFC 3164). This type has no effect on the kind of messages reported by the switch. However, it may be used by the syslog server to process messages, such as sorting or storing messages in the corresponding database. (Range: 16-23, Default: 23)

- **Logging Trap** – Limits log messages that are sent to the remote syslog server for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be sent to the remote server. (Range: 0-7, Default: 7)

- **Host IP Address** – Specifies the IP address of a remote server which will be sent syslog messages.

WEB INTERFACE

To configure the logging of error messages to remote servers:

1. Click System, Log, Remote Logs.
2. Enable remote logging, specify the facility type to use for the syslog messages. and enter the IP address of the remote servers.
3. Click Apply.

Figure 22: Configuring Settings for Remote Logging of Error Messages

SENDING SIMPLE MAIL TRANSFER PROTOCOL ALERTS

Use the System > Log > SMTP page to alert system administrators of problems by sending SMTP (Simple Mail Transfer Protocol) email messages when triggered by logging events of a specified level. The messages are sent to specified SMTP servers on the network and can be retrieved using POP or IMAP clients.

CLI REFERENCES

- "SMTP Alerts" on page 498

PARAMETERS

These parameters are displayed:

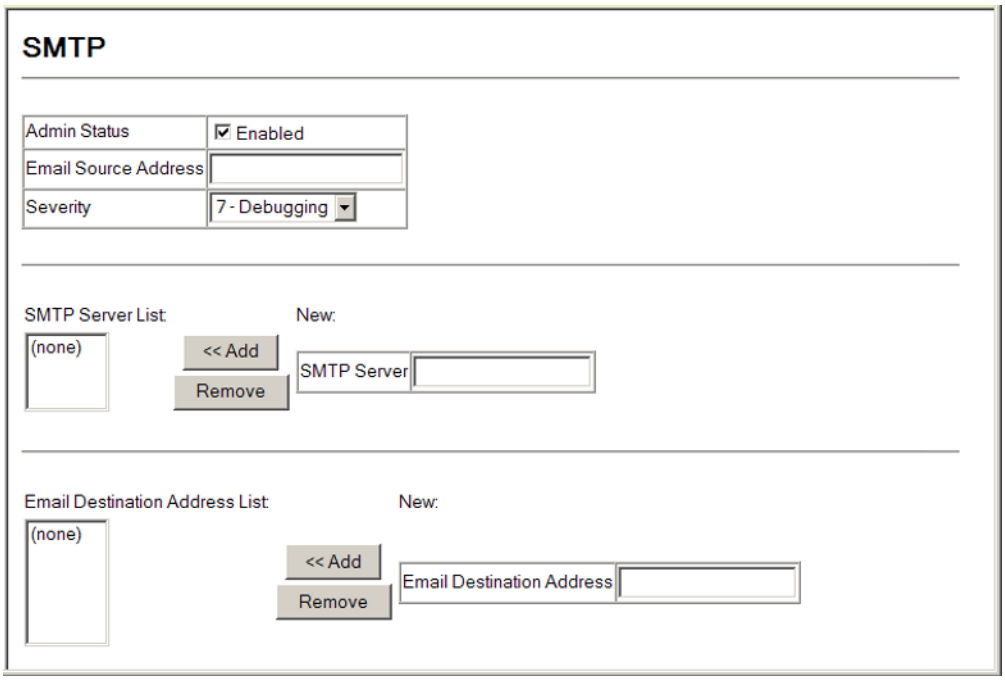
- **Admin Status** – Enables/disables the SMTP function. (Default: Enabled)
- **Email Source Address** – Sets the email address used for the "From" field in alert messages. You may use a symbolic email address that identifies the switch, or the address of an administrator responsible for the switch.
- **Severity** – Sets the syslog severity threshold level (see the table on page 123) used to trigger alert messages. All events at this level or higher will be sent to the configured email recipients. For example, using Level 7 will report all events from level 7 to level 0. (Default: Level 7)
- **SMTP Server List** – Specifies a list of up to three recipient SMTP servers. The switch attempts to connect to the other listed servers if the first fails. Use the New SMTP Server text field and the Add/Remove buttons to configure the list.
- **Email Destination Address List** – Specifies the email recipients of alert messages. You can specify up to five recipients.
- **Server IP Address** – Specifies a list of up to three recipient SMTP servers. The switch attempts to connect to the other listed servers if the first fails.

WEB INTERFACE

To configure SMTP alert messages:

1. Click System, Log, SMTP.
2. Enable SMTP, specify a source email address, and select the minimum severity level. Specify the source and destination email addresses, and one or more SMTP servers.
3. Click Apply.

Figure 23: Configuring SMTP Alert Messages



RESETTING THE SYSTEM

Use the System > Reset menu to restart the switch immediately, or after a specified delay.

CLI REFERENCES

- "reload (Privileged Exec)" on page 450
- "reload (Global Configuration)" on page 446
- "show reload" on page 451

COMMAND USAGE

- This command resets the entire system.
- When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory by the copy running-config startup-config command (see the copy command).

PARAMETERS

The following parameters are displayed in the web interface:

- **Hours** – Specifies the amount of hours to wait, combined with the minutes, before the switch resets. (Range: 0-576; Default: 0)
- **Minutes** – Specifies the amount of minutes to wait, combined with the hours, before the switch resets. (Range: 1-34560; Default: 0)

- **Reset** – Resets the switch after the specified time. If the hour and minute fields are blank, then the switch will reset immediately.
- **Refresh** – Refreshes the countdown timer of a pending delayed reset.
- **Cancel** – Cancels a pending delayed reset.

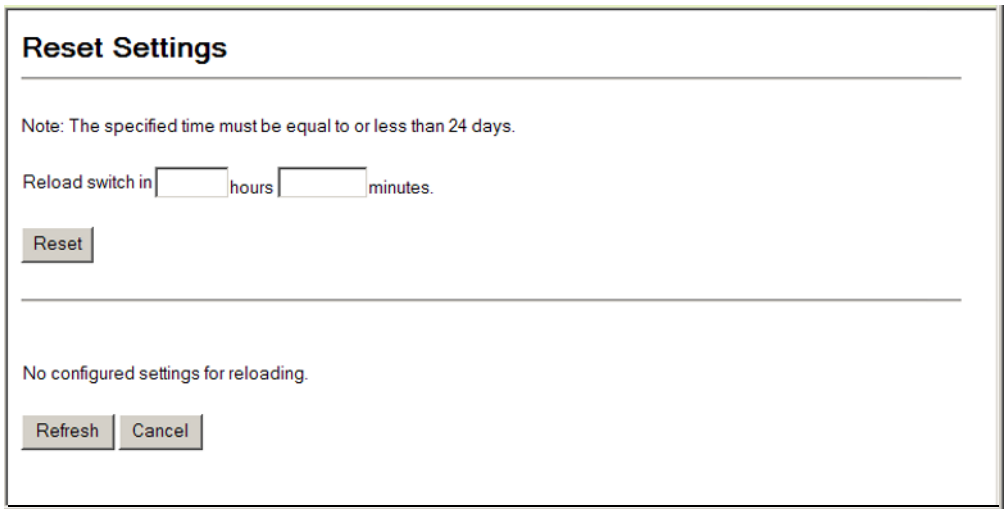
NOTE: To immediately restart the switch, enter "0" in both the Hours and Minutes fields, and click Reset.

WEB INTERFACE

To restart the switch:

1. Click System, then Reset.
2. Enter the amount of time the switch should wait before rebooting.
3. Click the Reset button to reboot the switch or click the Cancel button to cancel a configured reset.
4. If prompted, confirm that you want reset the switch or cancel a configured reset.

Figure 24: Restarting the Switch



SETTING THE SYSTEM CLOCK

Simple Network Time Protocol (SNTP) allows the switch to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. You can also manually set the clock. If the clock is not set manually or via SNTP, the switch will only record the time from the factory default set at the last bootup.

When the SNTP client is enabled, the switch periodically sends a request for a time update to a configured time server. You can configure up to three time server IP addresses. The switch will attempt to poll each server in the configured sequence.

SETTING THE TIME MANUALLY

Use the System > SNTP > Current Time page to set the system time on the switch manually without using SNTP.

CLI REFERENCES

- "calendar set" on page 514
- "show calendar" on page 515

PARAMETERS

The following parameters are displayed in the web interface:

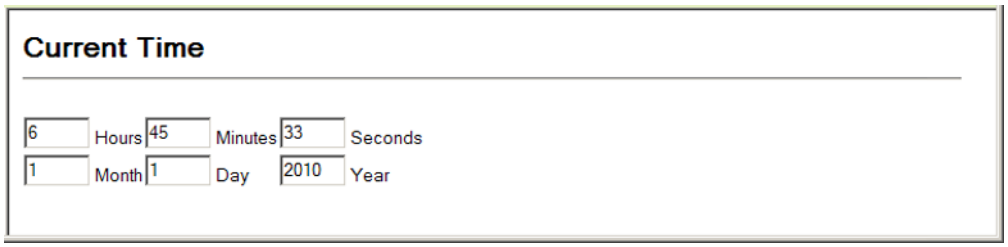
- **Current Time** – Shows the current time set on the switch.
- **Hours** – Sets the hour. (Range: 0-23; Default: 0)
- **Minutes** – Sets the minute value. (Range: 0-59; Default: 0)
- **Seconds** – Sets the second value. (Range: 0-59; Default: 0)
- **Month** – Sets the month. (Range: 1-12; Default: 1)
- **Day** – Sets the day of the month. (Range: 1-31; Default: 1)
- **Year** – Sets the year. (Range: 2001-2100; Default: 2001)

WEB INTERFACE

To manually set the system clock:

1. Click SNTP, then Current Time.
2. Enter the time and date in the appropriate fields.
3. Click Apply

Figure 25: Manually Setting the System Clock



CONFIGURING SNTP

Use the SNTP > Configuration page to configure the switch to send time synchronization requests to time servers by enabling SNTP client requests, setting the SNTP polling interval, and specifying the SNTP servers to use.

CLI REFERENCES

- "Time" on page 501

PARAMETERS

The following parameters are displayed in the web interface:

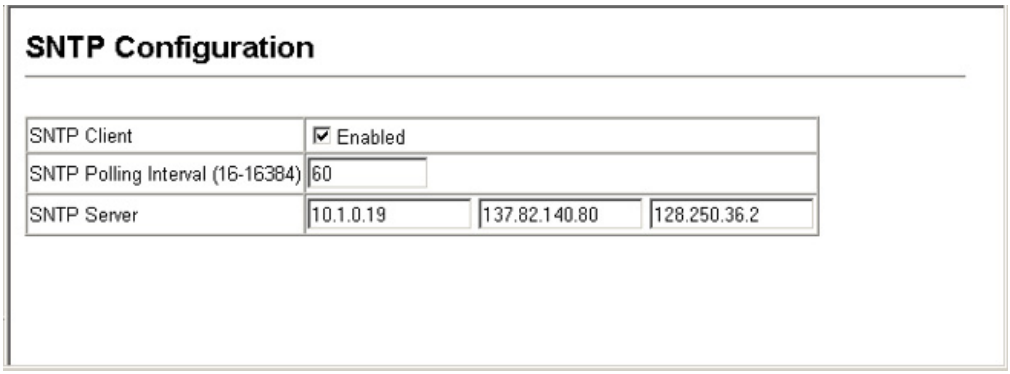
- **SNTP Client** – Configures the switch to operate as an SNTP client. This requires at least one NTP or SNTP time server to be specified in the SNTP Server field. (Default: Disabled)
- **SNTP Polling Interval** – Sets the interval between sending requests for a time update from a time server. (Range: 16-16384 seconds; Default: 16 seconds)
- **SNTP Server IP Address** – Sets the IP address for up to three time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence.

WEB INTERFACE

To configure SNTP:

1. Click SNTP, then Configuration.
2. Enable SNTP client requests, set the polling interval, and enter the IP address of up to three time servers.
3. Click Apply

Figure 26: Configuring SNTP



CONFIGURING NTP

The NTP client allows you to configure up to 50 NTP servers to poll for time updates. You can also enable authentication to ensure that reliable updates are received from only authorized NTP servers. The authentication keys and their associated key number must be centrally managed and manually distributed to NTP servers and clients. The key numbers and key values must match on both the server and client.

CLI REFERENCES

- "Time" on page 501

PARAMETERS

The following parameters are displayed in the web interface:

- **NTP Client** – Configures the switch to operate as an NTP client. This requires at least one time server to be specified in the NTP Server list. (Default: Disabled)
- **NTP Polling Interval** – Sets the interval between sending requests for a time update from NTP servers. (Fixed: 1024 seconds)
- **NTP Authenticate** – Enables authentication for time requests and updates between the switch and NTP servers. (Default: Disabled)
- **NTP Server** – Sets the IP address for an NTP server to be polled. The switch requests an update from all configured servers, then determines the most accurate time update from the responses received.
- **Version** – Specifies the NTP version supported by the server. (Fixed: Version 3)
- **Authenticate Key** – Specifies the number of the key in the NTP Authentication Key List to use for authentication with the configured server. The authentication key must match the key configured on the NTP server.
- **Key Number** – A number that specifies a key value in the NTP Authentication Key List. Up to 255 keys can be configured in the NTP Authentication Key List. Note that key numbers and values must match on both the server and client. (Range: 1-65535)

- **Key Context** – Specifies an MD5 authentication key string. The key string can be up to 32 case-sensitive printable ASCII characters (no spaces).

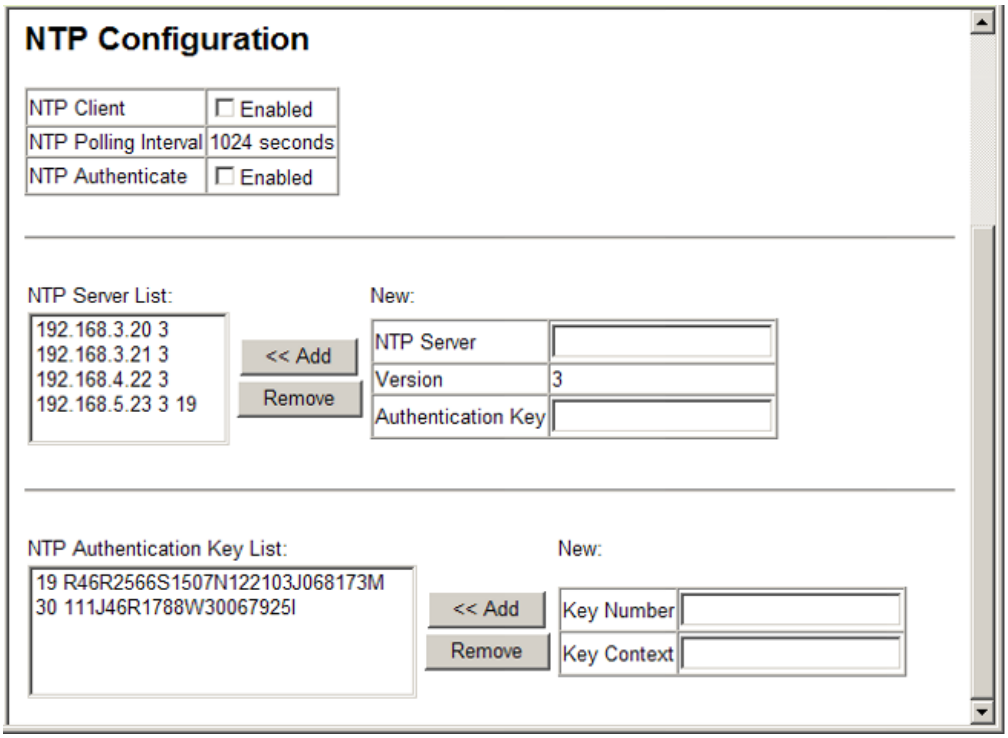
NOTE: SNTP and NTP clients cannot both be enabled at the same time.

WEB INTERFACE

To configure NTP:

1. Click SNTP, then Configuration.
2. Enable NTP client requests, set the polling interval, enable message authentication if required, and enter the IP address of up to 50 time servers.
3. Click Apply

Figure 27: Configuring NTP



SETTING THE TIME ZONE

Use the SNTP > Time Zone page to set the time zone. SNTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth's prime meridian, zero degrees longitude, which passes through Greenwich, England. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC. You can choose one of the 80 predefined time zone definitions, or your can manually configure the parameters for your local time zone.

CLI REFERENCES

- "clock timezone" on page 513
- "clock timezone-predefined" on page 513

PARAMETERS

The following parameters are displayed in the web interface:

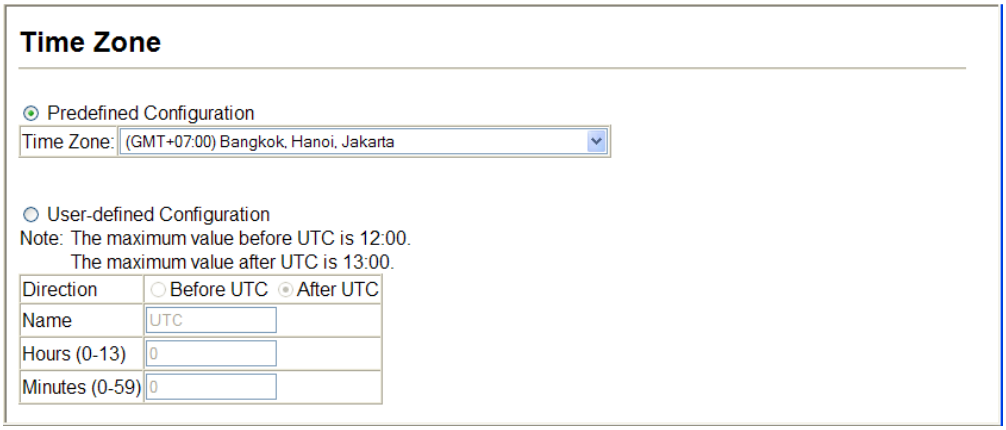
- **Predefined Configuration** – A drop-down box provides access to the 80 predefined time zone configurations. Each choice indicates it's offset from UTC and lists at least one major city or location covered by the time zone.
- **User-defined Configuration** – Allows the user to define all parameters of the local time zone.
  - **Direction**: Configures the time zone to be before (east of) or after (west of) UTC.
  - **Name** – Assigns a name to the time zone. (Range: 1-29 characters)
  - **Hours** (0-13) – The number of hours before/after UTC. The maximum value before UTC is 12. The maximum value after UTC is 13.
  - **Minutes** (0-59) – The number of minutes before/after UTC.

WEB INTERFACE

To set your local time zone:

1. Click SNTP, then Time Zone.
2. Set the offset for your time zone relative to the UTC in hours and minutes using either a predefined or custom definition.
3. Click Apply.

Figure 28: Setting the Time Zone



CONFIGURING SUMMER TIME

Use the Summer Time page to set the system clock forward during the summer months (also known as daylight savings time).

In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Summer Time, or Daylight Savings Time (DST). Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn.

CLI REFERENCES

- "Time" on page 501

PARAMETERS

The following parameters are displayed in the web interface:

General Configuration

- **Summer Time in Effect** – Shows if the system time has been adjusted.
- **Status** – Shows if summer time is set to take effect during the specified period.
- **Name** – Name of the time zone while summer time is in effect, usually an acronym. (Range: 1-30 characters)
- **Mode** – Selects one of the following configuration modes. (The Mode option can only be managed when the Summer Time Status option has been set to enabled for the switch.)

Predefined Mode – Configures the summer time status and settings for the switch using predefined configurations for several major regions of the world. To specify the time corresponding to your local time when summer time is in effect, select the predefined summer-time zone appropriate for your location.

Date Mode – Sets the start, end, and offset times of summer time for the switch on a one-time basis. This mode sets the summer-time zone relative

to the currently configured time zone. To specify a time corresponding to your local time when summer time is in effect, you must indicate the number of minutes your summer-time zone deviates from your regular time zone.

- **Offset** – Summer-time offset from the regular time zone, in minutes. (Range: 0-99 minutes)
- **From** – Start time for summer-time offset.
- **To** – End time for summer-time offset.

Recurring Mode – Sets the start, end, and offset times of summer time for the switch on a recurring basis. This mode sets the summer-time zone relative to the currently configured time zone. To specify a time corresponding to your local time when summer time is in effect, you must indicate the number of minutes your summer-time zone deviates from your regular time zone.

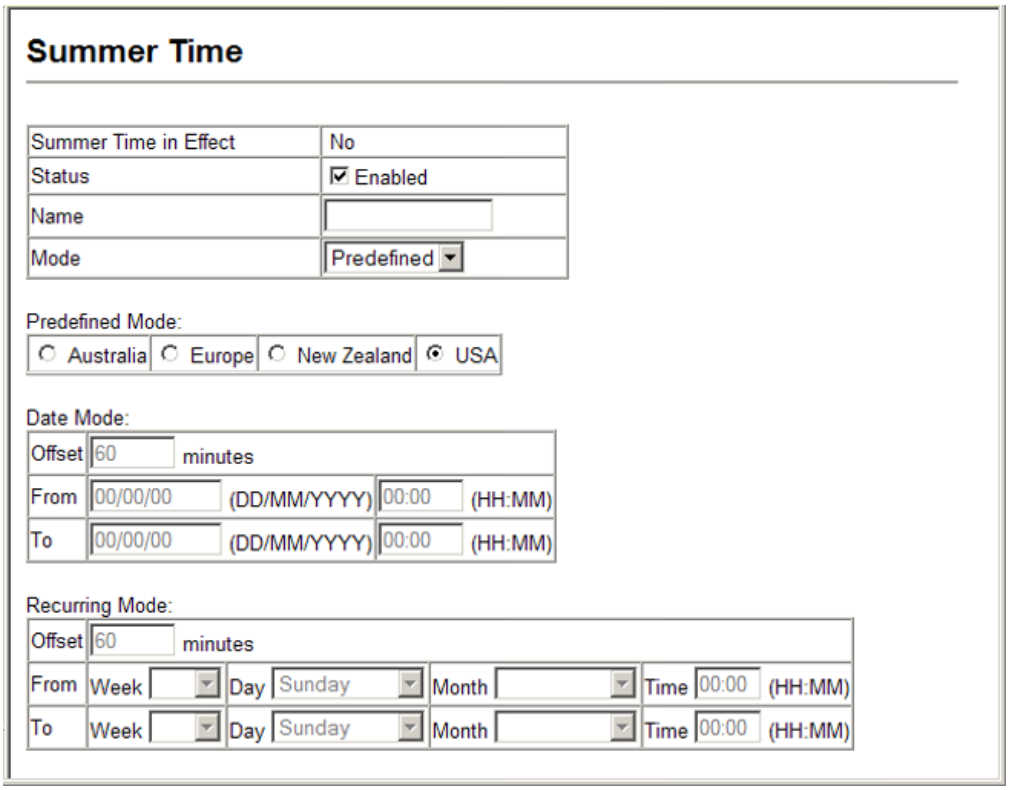
- **Offset** – Summer-time offset from the regular time zone, in minutes. (Range: 0-99 minutes)
- **From** – Start time for summer-time offset.
- **To** – End time for summer-time offset.

WEB INTERFACE

To specify summer time settings:

1. Click SNTP, Summer Time.
2. Select one of the configuration modes, configure the relevant attributes, enable summer time status.
3. Click Apply.

Figure 29: Configuring Summer Time



UPnP

Universal Plug and Play (UPnP) is a set of protocols that allows devices to connect seamlessly and simplifies the deployment of home and office networks. UPnP achieves this by issuing UPnP device control protocols designed upon open, Internet-based communication standards.

The first step in UPnP networking is discovery. When a device is added to the network, the UPnP discovery protocol allows that device to broadcast its services to control points on the network. Similarly, when a control point is added to the network, the UPnP discovery protocol allows that control point to search for UPnP enabled devices on the network.

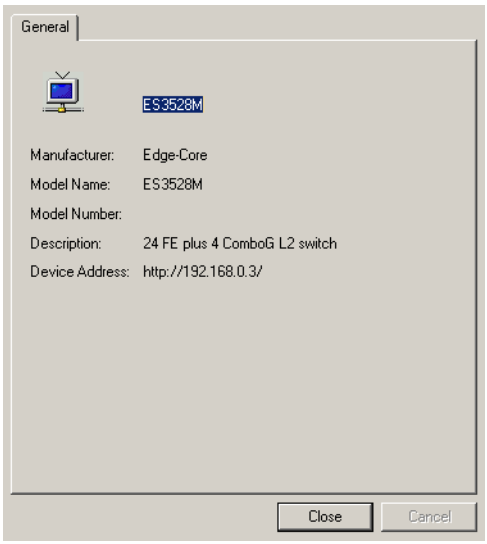
Once a control point has discovered a device its next step is to learn more about the device and its capabilities by retrieving the device's description from the URL provided by the device in the discovery message. After a control point has retrieved a description of the device, it can send actions to the device’s service. To do this, a control point sends a suitable control message to the control URL for the service (provided in the device description).

When a device is known to the control point, periodic event notification messages are sent. A UPnP description for a service includes a list of actions the service responds to and a list of variables that model the state of the service at run time.

If a device has a URL for presentation, then the control point can retrieve a page from this URL, load the page into a web browser, and depending on the capabilities of the page, allow a user to control the device and/or view device status.

Using UPnP under Windows XP – To access or manage the switch with the aid of UPnP under Windows XP, open My Network Places in the Explore file manager. An entry for "ES3552M" will appear in the list of discovered devices. Double-click on this entry to access the switch's web management interface. Or right-click on the entry and select "Properties" to display a list of device attributes advertised through UPnP.

Figure 30: Displaying UPnP Devices in Windows XP



UPnP CONFIGURATION

Use the UPnP > Configuration page to enable or disable UPnP, and to set advertisement and time out values.

CLI REFERENCES

- "UPnP" on page 523

PARAMETERS

The following parameters are displayed in the web interface:

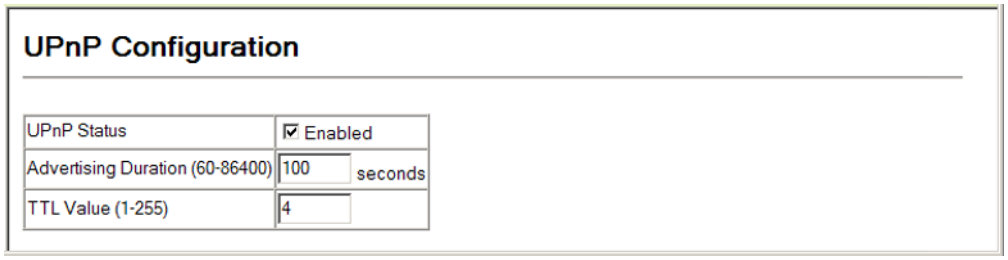
- **UPnP Status** – Enables/disables UPnP on the device. (Default: Disabled)
- **Advertising Duration** – This sets the duration of which a device will advertise its status to the control point. (Range: 60-86400 seconds; Default: 100 seconds)
- **TTL Value** – Sets the time-to-live (TTL) value for UPnP messages transmitted by the device. (Range: 1-255; Default: 4)

WEB INTERFACE

To configure UPnP:

1. Click UPnP, Configuration.
2. Enable UPnP, set the advertising duration and TTL value.
3. Click Apply.

Figure 31: Configuring UPnP



SWITCH CLUSTERING

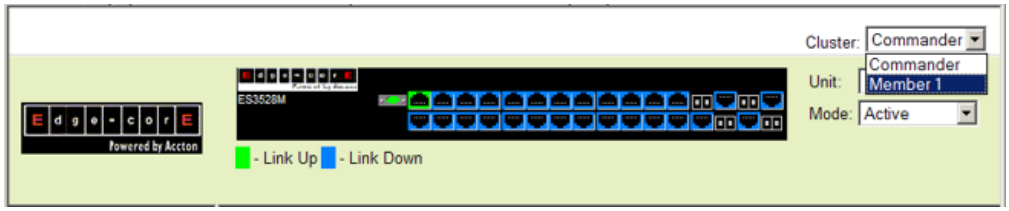
Switch clustering is a method of grouping switches together to enable centralized management through a single unit. Switches that support clustering can be grouped together regardless of physical location or switch type, as long as they are connected to the same local network.

COMMAND USAGE

- A switch cluster has a primary unit called the "Commander" which is used to manage all other "Member" switches in the cluster. The management station can use either Telnet or the web interface to communicate directly with the Commander through its IP address, and then use the Commander to manage Member switches through the cluster's "internal" IP addresses.
- Clustered switches must be in the same Ethernet broadcast domain. In other words, clustering only functions for switches which can pass information between the Commander and potential Candidates or active Members through VLAN 4093.
- Once a switch has been configured to be a cluster Commander, it automatically discovers other cluster-enabled switches in the network. These "Candidate" switches only become cluster Members when manually selected by the administrator through the management station.
- There can be up to 100 candidates and 36 member switches in one cluster.
- A switch can only be a member of one cluster.

- After the Commander and Members have been configured, any switch in the cluster can be managed from the web agent by choosing the desired Member ID from the Cluster drop down menu.

Figure 32: Choosing a Cluster Member to Manage



CONFIGURING GENERAL SETTINGS FOR CLUSTERS

Use the Administration > Cluster (Configure Global) page to create a switch cluster.

CLI REFERENCES

- "Switch Clustering" on page 518

COMMAND USAGE

First be sure that clustering is enabled on the switch (the default is disabled), then set the switch as a Cluster Commander. Set a Cluster IP Pool that does not conflict with the network IP subnet. Cluster IP addresses are assigned to switches when they become Members and are used for communication between Member switches and the Commander.

PARAMETERS

These parameters are displayed:

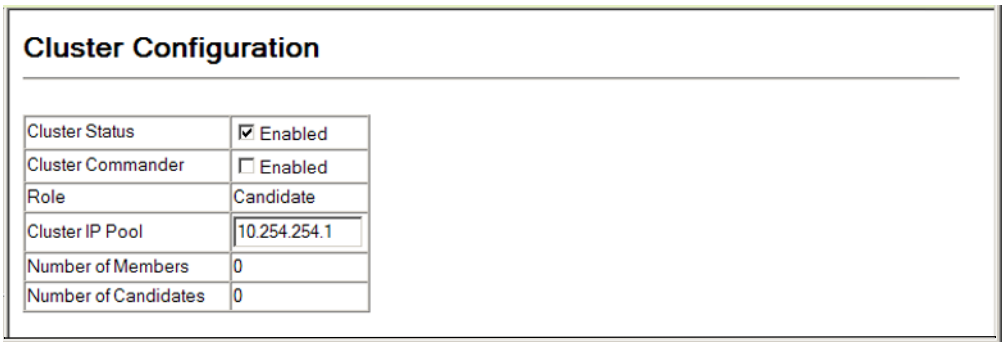
- **Cluster Status** – Enables or disables clustering on the switch. (Default: Enabled)
- **Commander Status** – Enables or disables the switch as a cluster Commander. (Default: Disabled)
- **Role** – Indicates the current role of the switch in the cluster; either Commander, Member, or Candidate. (Default: Candidate)
- **Cluster IP Pool** – An "internal" IP address pool that is used to assign IP addresses to Member switches in the cluster. Internal cluster IP addresses are in the form 10.x.x.member-ID. Only the base IP address of the pool needs to be set since Member IDs can only be between 1 and 36. Note that you cannot change the cluster IP pool when the switch is currently in Commander mode. Commander mode must first be disabled. (Default: 10.254.254.1)
- **Number of Members** – The current number of Member switches in the cluster.
- **Number of Candidates** – The current number of Candidate switches discovered in the network that are available to become Members.

WEB INTERFACE

To configure a switch cluster:

1. Click Cluster, Configuration.
2. Set the required attributes for a Commander or a managed candidate.
3. Click Apply

Figure 33: Configuring a Switch Cluster



CLUSTER MEMBER CONFIGURATION

Use the Cluster > Member Configuration page to add Candidate switches to the cluster as Members.

CLI REFERENCES

- "Switch Clustering" on page 518

PARAMETERS

These parameters are displayed:

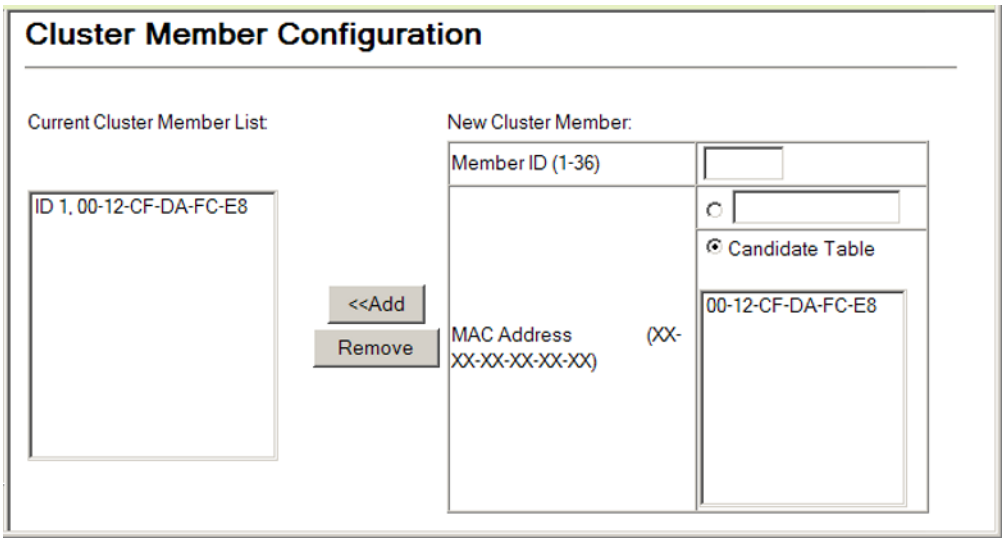
- **Member ID** – Specify a Member ID number for the selected Candidate switch. (Range: 1-36)
- **MAC Address** – Select a discovered switch MAC address from the Candidate Table, or enter a specific MAC address of a known switch.

WEB INTERFACE

To configure cluster members:

1. Click Cluster, Member Configuration.
2. Select one of the cluster candidates discovered by this switch, or enter the MAC address of a candidate.
3. Click Apply.

Figure 34: Configuring Cluster Members



DISPLAYING INFORMATION ON CLUSTER MEMBERS

Use the Cluster > Member Information page to display information on current cluster Member switches.

CLI REFERENCES

- "Switch Clustering" on page 518

PARAMETERS

These parameters are displayed:

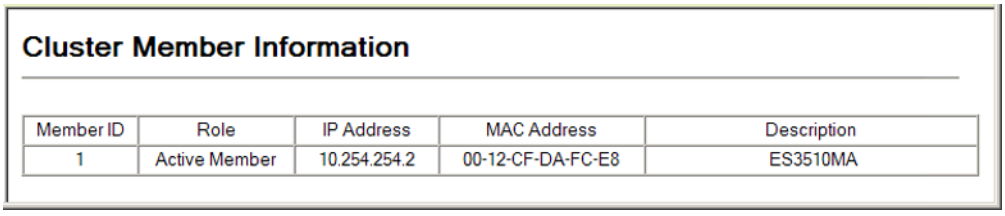
- **Member ID** – The ID number of the Member switch. (Range: 1-36)
- **Role** – Indicates the current status of the switch in the cluster.
- **IP Address** – The internal cluster IP address assigned to the Member switch.
- **MAC Address** – The MAC address of the Member switch.
- **Description** – The system description string of the Member switch.

WEB INTERFACE

To show the cluster members:

1. Click Cluster, Member Information.

Figure 35: Showing Cluster Members



CLUSTER CANDIDATE INFORMATION

Use the Cluster > Candidate Information page to display information about discovered switches in the network that are already cluster Members or are available to become cluster Members.

CLI REFERENCES

- "Switch Clustering" on page 518

PARAMETERS

These parameters are displayed:

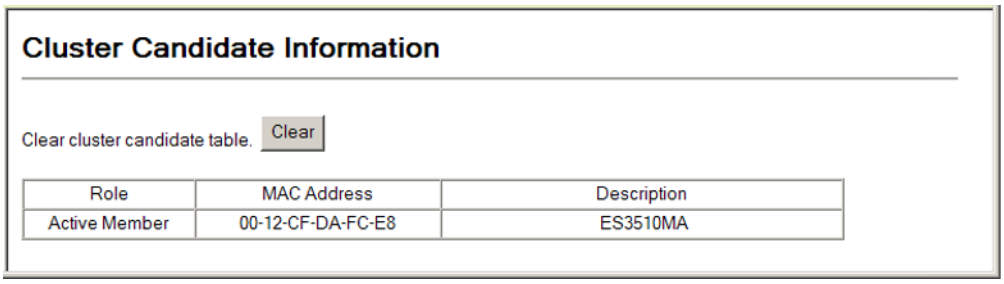
- **Role** – Indicates the current status of Candidate switches in the network.
- **MAC Address** – The MAC address of the Candidate switch.
- **Description** – The system description string of the Candidate switch.

WEB INTERFACE

To show cluster candidates:

1. Click Cluster, Candidate Information.

Figure 36: Showing Cluster Candidates



5 SIMPLE NETWORK MANAGEMENT PROTOCOL

This chapter describes the following topics:

- Community Access Strings – Configures the community strings authorized for management access by clients using SNMP v1 and v2c.
- Trap Managers and Trap Types – Specifies the host devices to be sent traps and the types of traps to send
- MAC Notification Traps – Sends a trap when dynamic addresses are added to or removed from the MAC address table.
- SNMP Agent – Enables SNMP service for all management clients.
- Local Engine ID – Changes the local engine ID.
- Remote Engine ID – Configures a engine ID for a remote management station.
- Local SNMPv3 Users – Authorizes management access for SNMPv3 clients, or to identify the source of SNMPv3 trap messages sent from the local switch.
- Remote SNMPv3 Users – Identifies the source of SNMPv3 inform messages sent from the local switch.
- SNMPv3 Groups – Adds an SNMPv3 group which can be used to set the access policy for its assigned users.
- SNMPv3 Views – Configures SNMPv3 views which are used to restrict user access to specified portions of the MIB tree.

OVERVIEW

Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. Equipment commonly managed with SNMP includes switches, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

Managed devices supporting SNMP contain software, which runs locally on the device and is referred to as an agent. A defined set of variables, known as managed objects, is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base

(MIB) that provides a standard presentation of the information controlled by the agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The switch includes an onboard agent that supports SNMP versions 1, 2c, and 3. This agent continuously monitors the status of the switch hardware, as well as the traffic passing through its ports. A network management station can access this information using network management software. Access to the onboard agent from clients using SNMP v1 and v2c is controlled by community strings. To communicate with the switch, the management station must first submit a valid community string for authentication.

Access to the switch from clients using SNMPv3 provides additional security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree.

The SNMPv3 security structure consists of security models, with each model having it's own security levels. There are three security models defined, SNMPv1, SNMPv2c, and SNMPv3. Users are assigned to "groups" that are defined by a security model and specified security levels. Each group also has a defined security access to set of MIB objects for reading and writing, which are known as "views." The switch has a default view (all MIB objects) and default groups defined for security models v1 and v2c. The following table shows the security models and levels available and the system default settings.

Table 9: SNMPv3 Security Models and Levels

Model	Level	Group	Read View	Write View	Notify View	Security
v1	noAuthNoPriv	public (read only)	defaultview	none	none	Community string only
v1	noAuthNoPriv	private (read/write)	defaultview	defaultview	none	Community string only
v1	noAuthNoPriv	*user defined*	*user defined*	*user defined*	*user defined*	Community string only
v2c	noAuthNoPriv	public (read only)	defaultview	none	none	Community string only
v2c	noAuthNoPriv	private (read/write)	defaultview	defaultview	none	Community string only
v2c	noAuthNoPriv	*user defined*	*user defined*	*user defined*	*user defined*	Community string only
v3	noAuthNoPriv	*user defined*	*user defined*	*user defined*	*user defined*	A user name match only
v3	AuthNoPriv	*user defined*	*user defined*	*user defined*	*user defined*	Provides user authentication via MD5 or SHA algorithms
v3	AuthPriv	*user defined*	*user defined*	*user defined*	*user defined*	Provides user authentication via MD5 or SHA algorithms and data privacy using DES 56-bit encryption

NOTE: The predefined default groups and view can be deleted from the system. You can then define customized groups and views for the SNMP clients that require access.

COMMAND USAGE

Configuring SNMPv1/2c Management Access

To configure SNMPv1 or v2c management access to the switch, follow these steps:

1. Use the SNMP > Configuration page to configure the community strings authorized for management access, to enable trap messages, and to specify trap managers so that key events are reported by this switch to your management station.

2. Use the SNMP > Agent Status page to enable SNMP on the switch.

Configuring SNMPv3 Management Access

1. Use the SNMP > Configuration page to configure the community strings authorized for management access, to enable trap messages, and to specify trap managers so that key events are reported by this switch to your management station.

2. Use the SNMP > SNMPv3 > Engine ID page to change the local engine ID. If you want to change the default engine ID, it must be changed before configuring other parameters.

3. Use the SNMP > SNMPv3 > Views page to specify read and write access views for the switch MIB tree.

4. Use the SNMP > SNMPv3 > Users page to configure SNMP user groups with the required security model (i.e., SNMP v1, v2c or v3) and security level (i.e., authentication and privacy).

5. Use the SNMP > SNMPv3 > Groups page to assign SNMP users to groups, along with their specific authentication and privacy passwords.

6. Use the SNMP > Agent Status page to enable SNMP on the switch.

SETTING COMMUNITY ACCESS STRINGS

Use the SNMP > Configuration page to configure up to five community strings authorized for management access by clients using SNMP v1 and v2c. For security reasons, you should consider removing the default strings.

CLI REFERENCES

- "snmp-server community" on page 529

PARAMETERS

These parameters are displayed:

- **Community String** – A community string that acts like a password and permits access to the SNMP protocol.

  Range: 1-32 characters, case sensitive
  Default strings: "public" (Read-Only), "private" (Read/Write)

- **Access Mode** – Specifies the access rights for the community string:

  - **Read-Only** – Authorized management stations are only able to retrieve MIB objects.
  - **Read/Write** – Authorized management stations are able to both retrieve and modify MIB objects.

WEB INTERFACE

To set a community access string:

1. Click SNMP, Configuration.
2. Add new community strings as required, and select the corresponding access rights from the Access Mode list.
3. Click Apply

Figure 37: Setting Community Access Strings

SPECIFYING TRAP MANAGERS AND TRAP TYPES

Use the SNMP > Configuration page specify the host devices to be sent traps and the types of traps to send. Traps indicating status changes are issued by the switch to the specified trap managers. You must specify trap managers so that key events are reported by this switch to your management station (using network management software). You can specify up to five management stations that will receive authentication failure messages and other trap messages from the switch.

CLI REFERENCES

- "snmp-server host" on page 540
- "snmp-server enable traps" on page 539

COMMAND USAGE

- Notifications are issued by the switch as trap messages by default. The recipient of a trap message does not send a response to the switch. Traps are therefore not as reliable as inform messages, which include a request for acknowledgement of receipt. Informs can be used to ensure that critical information is received by the host. However, note that informs consume more system resources because they must be kept in memory until a response is received. Informs also add to network traffic. You should consider these effects when deciding whether to issue notifications as traps or informs.

  To send an inform to a SNMPv2c host, complete these steps:

  1. Enable the SNMP agent (page 151).
  2. Create a view with the required notification messages (page 162).
  3. Configure the group (matching the community string specified on the SNMP > Configuration page) to include the required notify view (page 158).
  4. Enable trap informs as described in the following pages.

  To send an inform to a SNMPv3 host, complete these steps:

  1. Enable the SNMP agent (page 151).
  2. Create a local SNMPv3 user to use in the message exchange process (page 154). If the user specified in the trap configuration page does not exist, an SNMPv3 group will be automatically created using the name of the specified local user, and default settings used for the read, write, and notify view.
  3. Create a view with the required notification messages (page 162).
  4. Create a group that includes the required notify view (page 158).
  5. Enable trap informs as described in the following pages.

PARAMETERS

These parameters are displayed:

- **Trap Manager Capability** – This switch supports up to five trap managers.
- **Trap Manager IP Address** – IP address of a new management station to receive notification messages (i.e., the targeted recipient).
- **Trap Manager Community String** – Specifies a valid community string for the new trap manager entry. (Range: 1-32 characters, case sensitive)

  Although you can set this string in the Trap Managers table, we recommend that you define this string in the SNMP Community section at the top of the SNMP Configuration page (for Version 1 or 2c clients), or define a corresponding "User Name" in the SNMPv3 > Users page or SNMPv3 > Remote Users page (for Version 3 clients).

  When sending SNMPv3 trap messages, the community string is used as the name of a local user to identify the source of the trap messages sent from this switch. If an account for the specified user has not been created (page 154), one will be automatically generated.

  When sending SNMPv3 inform messages, the community string is used as the name of a remote user to identify the source of the inform messages sent from this switch. An account for the specified user must be manually configured (page 155).
- **Trap UDP Port** – Specifies the UDP port number used by the trap manager. (Default: 162)
- **Trap Version** – Specifies whether to send notifications as SNMP v1, v2c, or v3 traps. (Default: v1)
- **Trap Security Level** – When trap version 3 is selected, you must specify one of the following security levels. (Default: noAuthNoPriv)
  - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications.
  - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.
  - **AuthPriv** – SNMP communications use both authentication and encryption.
- **Inform** – Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: Notifications are sent as trap messages)
  - **Timeout** – The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)
  - **Retry times** – The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)

- **Enable Authentication Traps**[2] – Issues a notification message to specified IP trap managers whenever an invalid community string is submitted during the SNMP access authentication process. (Default: Enabled)

- **Enable User Authentication Traps** – Issues user login authentication failure or success notifications. (Default: Enabled)

  For more information on configuring user login authentication, see "Configuring Local/Remote Logon Authentication" on page 171.

- **Enable Link-up and Link-down Traps**[2] – Issues a notification message whenever a port link is established or broken. (Default: Enabled)

- **Enable MAC Notification Traps**[3] – Globally enables traps when changes occur for dynamic addresses in the MAC address table.

  Dynamic entries stored in the address table are determined by examining the source address of ingress packets. This command is used to generate SNMP traps when a dynamic address is added to or removed from the MAC address table of an interface for which MAC notification traps have been enabled on the SNMP > Port/Trunk Configuration page (see "Configuring MAC Notification Traps for Interfaces").

  Changes to dynamic address entries in the MAC address table may occur due to address aging, changes in spanning tree topology, or for other reasons. Changes to static address entries are not included in this type of trap message.

  The attributes reported in these traps include the (1) MAC address, (2) VLAN identifier, (3) interface index, (4) and an ADD/REMOVE attribute indicating the type of change.

  - **Interval** – The delay between sending two consecutive trap messages. (Range: 0-3600 seconds; Default: 1 second)

    If the **interval** parameter is set to a non-zero value, trap messages will be stored in a buffer, and sent when the interval expires. The buffer can hold up to 512 messages. Note that some notifications may be lost if the buffer overflows during the specified interval.

WEB INTERFACE

To configure trap managers:

1. Click SNMP, Configuration.

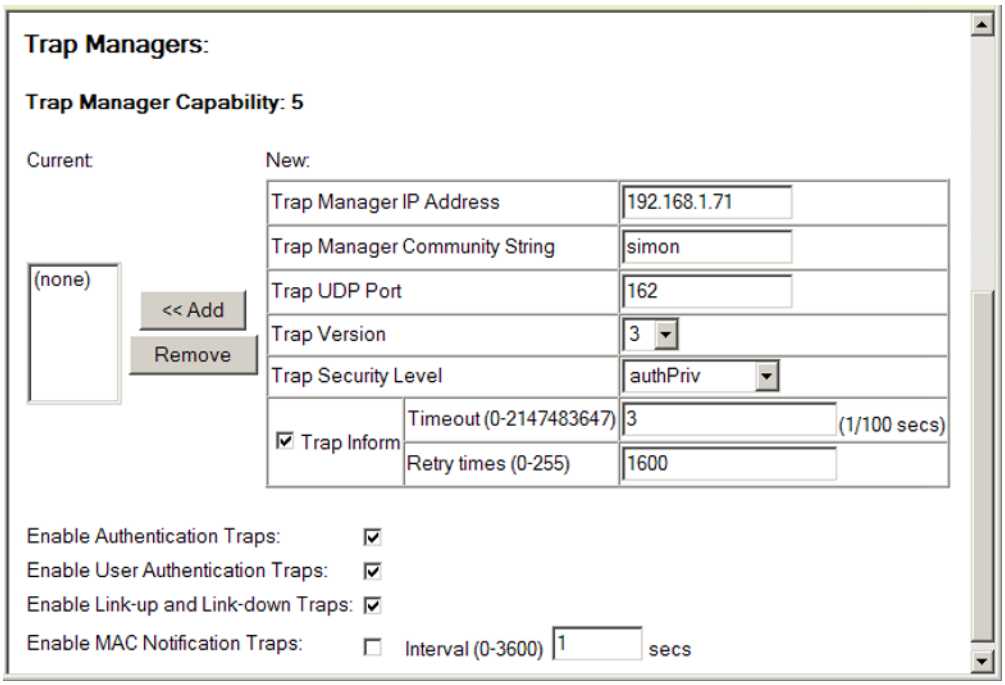
2. Enter the IP address and community string for each management station that will receive trap messages, specify the UDP port, trap version, trap security level (for v3 clients), trap inform settings (for v2c/v3 clients), and then click Add.

2. These are legacy notifications and therefore when used for SNMPv3 hosts, they must be enabled in conjunction with the corresponding entries in SNMPv3 Views (page 162).
3. MAC notification traps must also be configured at the interface level using the snmp-server enable port-traps mac-notification command.

3. Select the trap types required using the check boxes.

4. Click Apply

Figure 38: Configuring Trap Managers



CONFIGURING MAC NOTIFICATION TRAPS FOR INTERFACES

Use the SNMP > Port/Trunk Configuration pages to send a trap when dynamic addresses are added to or removed from the MAC address table for an interface.

CLI REFERENCES

- "snmp-server enable port-traps mac-notification" on page 543

COMMAND USAGE

MAC notification traps must also be globally enabled on the SNMP > Configuration page for this interface-level command to take effect (see "Specifying Trap Managers and Trap Types").

PARAMETERS

These parameters are displayed:

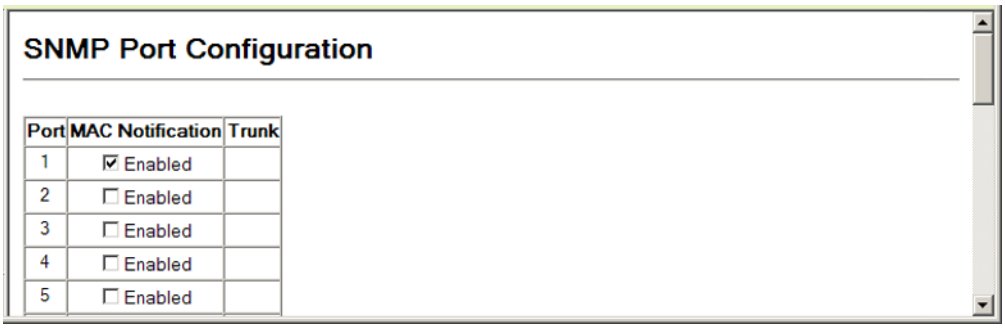
- **Port** – Port number. (Range: 1-28/52)
- **MAC Notification** – Send trap messages when dynamic addresses are added to or removed from the MAC address table for this interface.
- **Trunk** – Shows if this port is a member of a trunk.

WEB INTERFACE

To configure MAC Notification traps for interfaces:

1. Click SNMP, then Port Configuration or Trunk Configuration.
2. Mark the MAC Notification check box for those interfaces on which MAC Notification traps are to be enabled.
3. Click Apply

Figure 39: Configuring MAC Notification for Interfaces



ENABLING THE SNMP AGENT

Use the SNMP > Agent Status page to enable SNMP service for all management clients (i.e., versions 1, 2c, 3).

CLI REFERENCES

- "snmp-server" on page 528

PARAMETERS

These parameters are displayed:

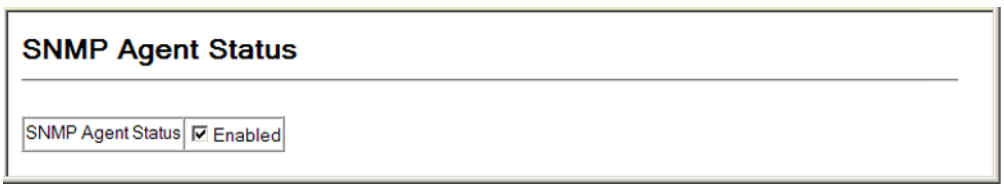
- **Agent Status** – Enables SNMP on the switch. (Default: Enabled)

WEB INTERFACE

To enable SNMP service:

1. Click SNMP, Agent Status.
2. Enable SNMP service.
3. Click Apply

Figure 40: Enabling the SNMP Agent



SETTING THE LOCAL ENGINE ID

Use the SNMP > SNMPv3 > Engine ID page to change the local engine ID. An SNMPv3 engine is an independent SNMP agent that resides on the switch. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.

CLI REFERENCES

- "snmp-server engine-id" on page 531

COMMAND USAGE

- A local engine ID is automatically generated that is unique to the switch. This is referred to as the default engine ID. If the local engine ID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users.

PARAMETERS

These parameters are displayed:

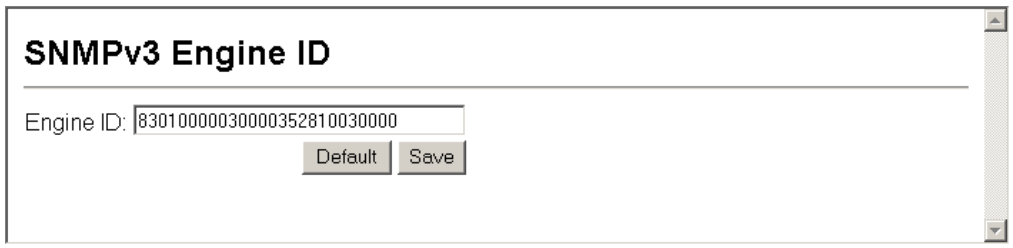
- **Engine ID** – A new engine ID can be specified by entering 9 to 64 hexadecimal characters (5 to 32 octets in hexadecimal format). If an odd number of characters are specified, a trailing zero is added to the value to fill in the last octet. For example, the value "123456789" is equivalent to "1234567890".

WEB INTERFACE

To configure the local SNMP engine ID:

1. Click SNMP, SNMPv3, Engine ID.
2. Enter an ID of a least 9 hexadecimal characters.
3. Click Apply

Figure 41: Configuring the Local Engine ID for SNMP



SPECIFYING A REMOTE ENGINE ID

Use the SNMP > SNMPv3 > Remote Engine ID) page to configure a engine ID for a remote management station. To allow management access from an SNMPv3 user on a remote device, you must first specify the engine identifier for the SNMP agent on the remote device where the user resides. The remote engine ID is used to compute the security digest for authentication and encryption of packets passed between the switch and a user on the remote host.

CLI REFERENCES

- "snmp-server engine-id" on page 531

COMMAND USAGE

- SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it. (See "Configuring Remote SNMPv3 Users.")

PARAMETERS

These parameters are displayed:

- **Remote Engine ID** – The engine ID can be specified by entering 9 to 64 hexadecimal characters (5 to 32 octets in hexadecimal format). If an odd number of characters are specified, a trailing zero is added to the value to fill in the last octet. For example, the value "123456789" is equivalent to "1234567890".

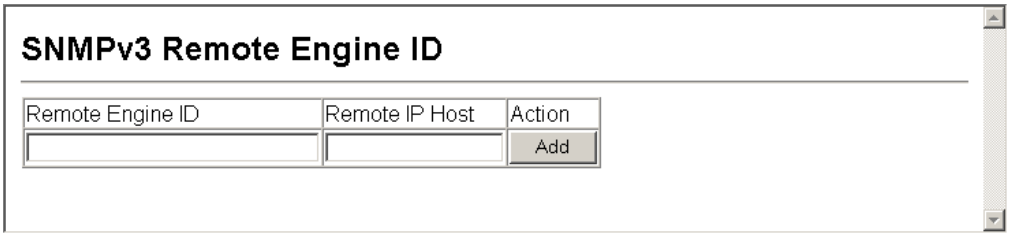
- **Remote IP Host** – The IP address of a remote management station which is using the specified engine ID.

WEB INTERFACE

To configure a remote SNMP engine ID:

1. Click SNMP, SNMPv3, Remote Engine ID.
2. Enter an ID of a least 9 hexadecimal characters, and the IP address of the remote host.
3. Click Apply

Figure 42: Configuring a Remote Engine ID for SNMP



CONFIGURING LOCAL SNMPV3 USERS

Use the SNMP > SNMPv3 > Users page to authorize management access for SNMPv3 clients, or to identify the source of SNMPv3 trap messages sent from the local switch. Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read, write, and notify view.

CLI REFERENCES

- "snmp-server user" on page 534

PARAMETERS

These parameters are displayed:

- **User Name** – The name of user connecting to the SNMP agent. (Range: 1-32 characters)
- **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- **Security Model** – The user security model; SNMP v1, v2c or v3.
- **Security Level** – The following security levels are only used for the groups assigned to the SNMP security model:
  - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications. (This is the default security level.)
  - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.
  - **AuthPriv** – SNMP communications use both authentication and encryption.
- **Authentication Protocol** – The method used for user authentication. (Options: MD5, SHA; Default: MD5)
- **Authentication Password** – A minimum of eight plain text characters is required.
- **Privacy Protocol** – The encryption algorithm use for data privacy; only 56-bit DES is currently available.
- **Privacy Password** – A minimum of eight plain text characters is required.

WEB INTERFACE

To configure a local SNMPv3 user:

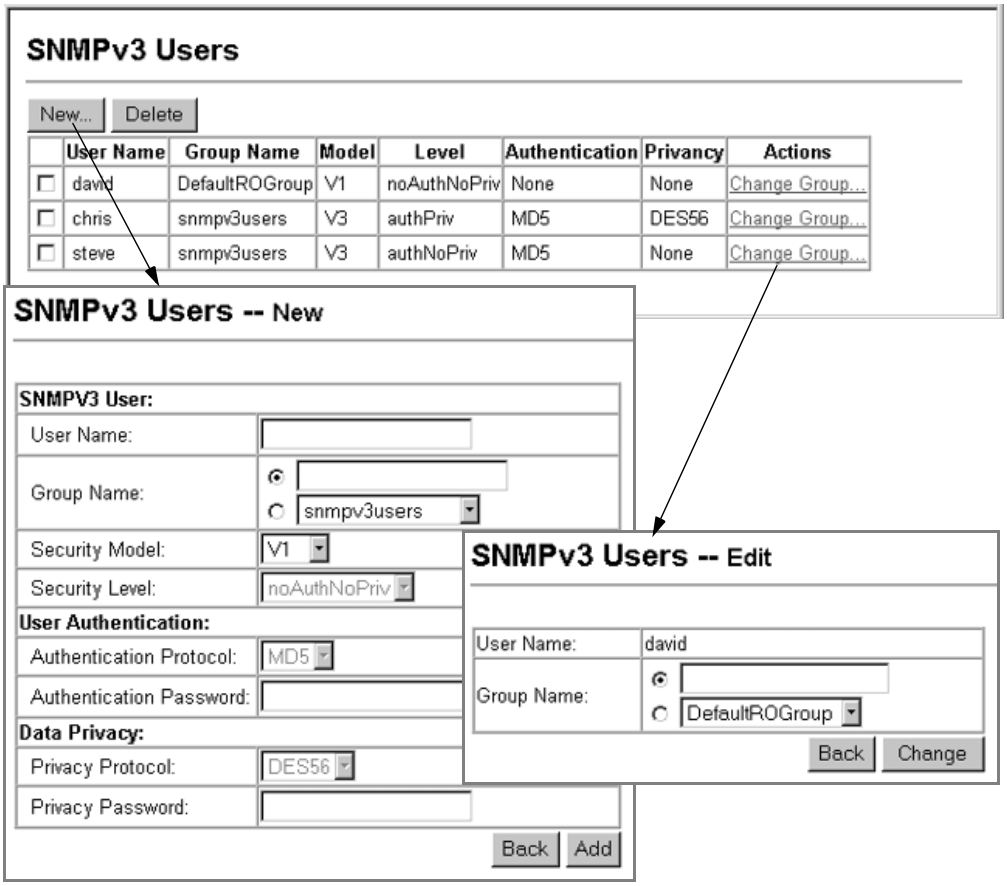
1. Click SNMP, SNMPv3, Users.

2. Click New to add a user.

3. Enter a name and assign it to a group. If the security model is set to SNMPv3 and the security level is authNoPriv or authPriv, then an authentication protocol and password must be specified. If the security level is authPriv, a privacy password must also be specified.

4. Click Add.

Figure 43: Configuring Local SNMPv3 Users



CONFIGURING REMOTE SNMPV3 USERS

Use the SNMP > SNMPv3 > Remote Users page to identify the source of SNMPv3 inform messages sent from the local switch. Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read, write, and notify view.

CLI REFERENCES

- "snmp-server user" on page 534

COMMAND USAGE

- To grant management access to an SNMPv3 user on a remote device, you must first specify the engine identifier for the SNMP agent on the remote device where the user resides. The remote engine ID is used to compute the security digest for authentication and encryption of packets passed between the switch and the remote user. (See "Specifying Trap Managers and Trap Types" and "Specifying a Remote Engine ID.")

PARAMETERS

These parameters are displayed:

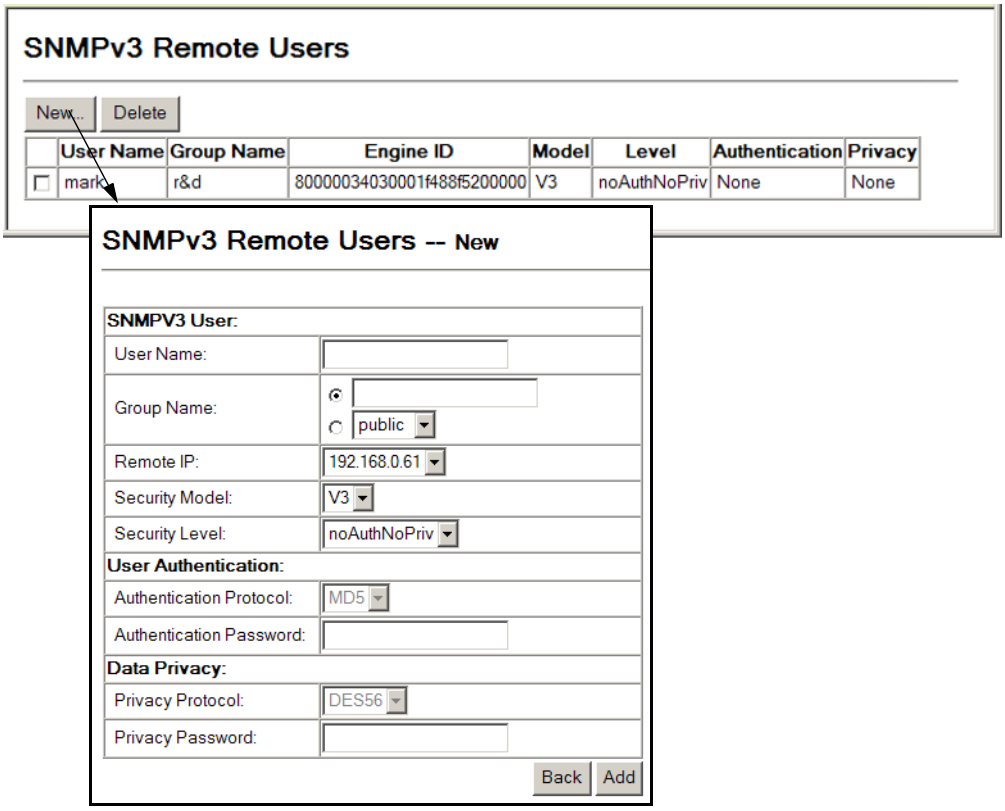
- **User Name** – The name of user connecting to the SNMP agent. (Range: 1-32 characters)
- **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- **Remote IP** – The Internet address of the remote device where the user resides.
- **Security Model** – The user security model. (SNMPv3 only)
- **Security Level** – The following security levels are only used for the groups assigned to the SNMP security model:
  - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications. (This is the default security level.)
  - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.
  - **AuthPriv** – SNMP communications use both authentication and encryption.
- **Authentication Protocol** – The method used for user authentication. (Options: MD5, SHA; Default: MD5)
- **Authentication Password** – A minimum of eight plain text characters is required.
- **Privacy Protocol** – The encryption algorithm use for data privacy; only 56-bit DES is currently available.
- **Privacy Password** – A minimum of eight plain text characters is required.

WEB INTERFACE

To configure a remote SNMPv3 user:

1. Click SNMP, SNMPv3, Remote Users.
2. Click New to add a user.
3. Enter a name and assign it to a group. Enter the IP address to identify the source of SNMPv3 inform messages sent from the local switch. If the security model is set to SNMPv3 and the security level is authNoPriv or authPriv, then an authentication protocol and password must be specified. If the security level is authPriv, a privacy password must also be specified.
4. Click Add.

Figure 44: Configuring Remote SNMPv3 Users



CONFIGURING SNMPV3 GROUPS

Use the SNMP > SNMPv3 > Groups page to add an SNMPv3 group which can be used to set the access policy for its assigned users, restricting them to specific read, write, and notify views. You can use the pre-defined default groups or create new groups to map a set of SNMP users to SNMP views.

CLI REFERENCES

- "show snmp group" on page 537

PARAMETERS

These parameters are displayed:

- **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- **Security Model** – The user security model; SNMP v1, v2c or v3.
- **Security Level** – The following security levels are only used for the groups assigned to the SNMP security model:
  - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications. (This is the default security level.)
  - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.
  - **AuthPriv** – SNMP communications use both authentication and encryption.
- **Read View** – The configured view for read access. (Range: 1-64 characters)
- **Write View** – The configured view for write access. (Range: 1-64 characters)
- **Notify View** – The configured view for notifications. (Range: 1-64 characters)

Table 10: Supported Notification Messages

Model	Level	Group
RFC 1493 Traps		
newRoot	1.3.6.1.2.1.17.0.1	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer immediately subsequent to its election.
topologyChange	1.3.6.1.2.1.17.0.2	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Discarding state. The trap is not sent if a newRoot trap is sent for the same transition.
SNMPv2 Traps		
coldStart	1.3.6.1.6.3.1.1.5.1	A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.
warmStart	1.3.6.1.6.3.1.1.5.2	A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.
linkDown*	1.3.6.1.6.3.1.1.5.3	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.
linkUp*	1.3.6.1.6.3.1.1.5.4	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.
authenticationFailure*	1.3.6.1.6.3.1.1.5.5	An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.
RMON Events (V2)		
risingAlarm	1.3.6.1.2.1.16.0.1	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps.
fallingAlarm	1.3.6.1.2.1.16.0.2	The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps.

Table 10: Supported Notification Messages (Continued)

Model	Level	Group
Private Traps		
swPowerStatus ChangeTrap	1.3.6.1.4.1.259.6.10.94.2.1.0.1	This trap is sent when the power state changes.
swPortSecurityTrap	1.3.6.1.4.1.259.6.10.94.2.1.0.36	This trap is sent when the port is being intruded. This trap will only be sent when the portSecActionTrap is enabled.
swIpFilterRejectTrap	1.3.6.1.4.1.259.6.10.94.2.1.0.40	This trap is sent when an incorrect IP address is rejected by the IP Filter.
swAuthenticationFailure	1.3.6.1.4.1.259.6.10.94.2.1.0.66	This trap will be triggered if authentication fails.
swAuthenticationSuccess	1.3.6.1.4.1.259.6.10.94.2.1.0.67	This trap will be triggered if authentication is successful.
swAtcBcastStormAlarmFireTrap	1.3.6.1.4.1.259.6.10.94.2.1.0.70	When broadcast traffic is detected as a storm, this trap is fired.
swAtcBcastStormAlarmClearTrap	1.3.6.1.4.1.259.6.10.94.2.1.0.71	When a broadcast storm is detected as normal traffic, this trap is fired.
swAtcBcastStormTcApplyTrap	1.3.6.1.4.1.259.6.10.94.2.1.0.72	When ATC is activated, this trap is fired.
swAtcBcastStormTcReleaseTrap	1.3.6.1.4.1.259.6.10.94.2.1.0.73	When ATC is released, this trap is fired.
swAtcMcastStormAlarmFireTrap	1.3.6.1.4.1.259.6.10.94.2.1.0.74	When multicast traffic is detected as the storm, this trap is fired.
swAtcMcastStormAlarmClearTrap	1.3.6.1.4.1.259.6.10.94.2.1.0.75	When multicast storm is detected as normal traffic, this trap is fired.
swAtcMcastStormTcApplyTrap	1.3.6.1.4.1.259.6.10.94.2.1.0.76	When ATC is activated, this trap is fired.
swAtcMcastStormTcReleaseTrap	1.3.6.1.4.1.259.6.10.94.2.1.0.77	When ATC is released, this trap is fired.
swLoopbackDetectionTrap	1.3.6.1.4.1.259.6.10.94.2.1.0.92	This trap is sent when loopback BPDUs have been detected.
networkAccessPortLinkDetectionTrap	1.3.6.1.4.1.259.6.10.94.2.1.0.96	This trap is sent when a networkAccessPortLinkDetection event is triggered.
autoUpgradeTrap	1.3.6.1.4.1.259.6.10.94.2.1.0.104	This trap is sent when auto upgrade is executed.
swCpuUtiRisingNotification	1.3.6.1.4.1.259.6.10.94.2.1.0.107	This notification indicates that the CPU utilization has risen from cpuUtiFallingThreshold to cpuUtiRisingThreshold.
swCpuUtiFallingNotification	1.3.6.1.4.1.259.6.10.94.2.1.0.108	This notification indicates that the CPU utilization has fallen from cpuUtiRisingThreshold to cpuUtiFallingThreshold.
swMemoryUtiRisingThreshold Notification	1.3.6.1.4.1.259.6.10.94.2.1.0.109	This notification indicates that the memory utilization has risen from memoryUtiFallingThreshold to memoryUtiRisingThreshold.

Table 10: Supported Notification Messages (Continued)

Model	Level	Group
swMemoryUtiFallingThreshold Notification	1.3.6.1.4.1.259.6.10.94.2.1.0.110	This notification indicates that the memory utilization has fallen from memoryUtiRisingThreshold to memoryUtiFallingThreshold.
dhcpRougeServerAttackTrap	1.3.6.1.4.1.259.6.10.94.2.1.0.114	This trap is sent when receiving a DHCP packet from a rouge server.
macNotificationTrap	1.3.6.1.4.1.259.6.10.94.2.1.0.138	This trap is sent when there are changes to a dynamic MAC address on the switch.

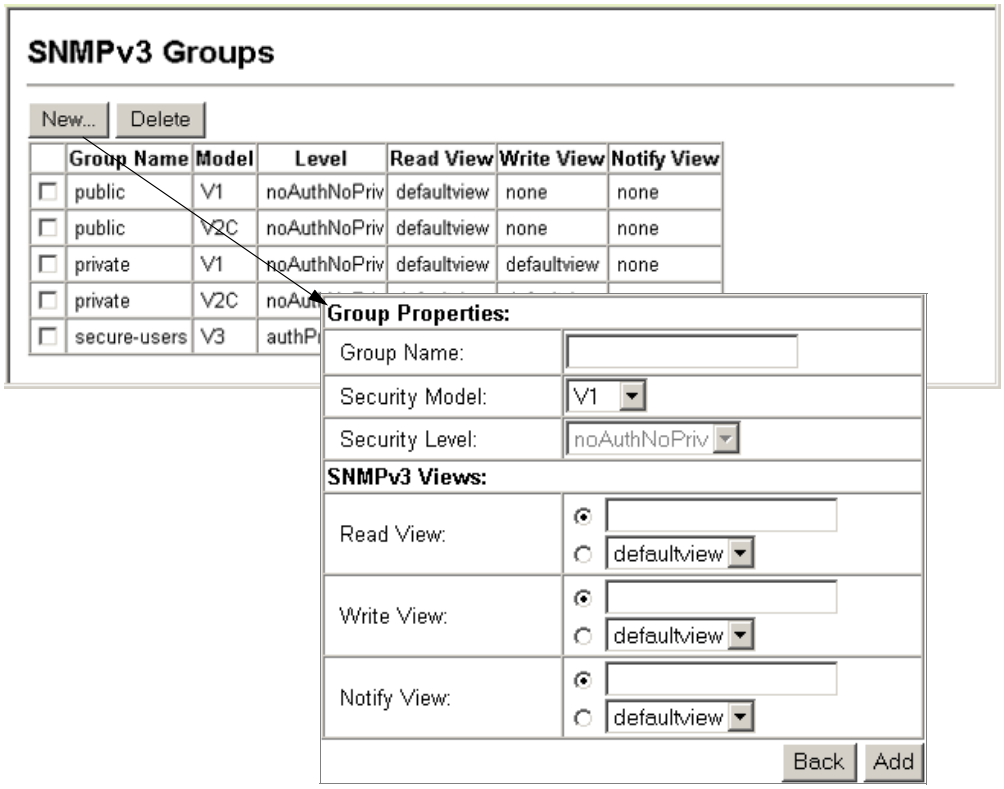
* These are legacy notifications and therefore must be enabled in conjunction with the corresponding traps on the SNMP Configuration menu.

WEB INTERFACE

To configure an SNMP group:

1. Click SNMP, SNMPv3, Groups.
2. Enter a group name, assign a security model and level, and then select read, write, and notify views.
3. Click Apply

Figure 45: Creating an SNMP Group



SETTING SNMPV3 VIEWS

Use the SNMP > SNMPv3 > Views page to configure SNMPv3 views which are used to restrict user access to specified portions of the MIB tree. The predefined view "defaultview" includes access to the entire MIB tree.

CLI REFERENCES

- "snmp-server view" on page 535

PARAMETERS

These parameters are displayed:

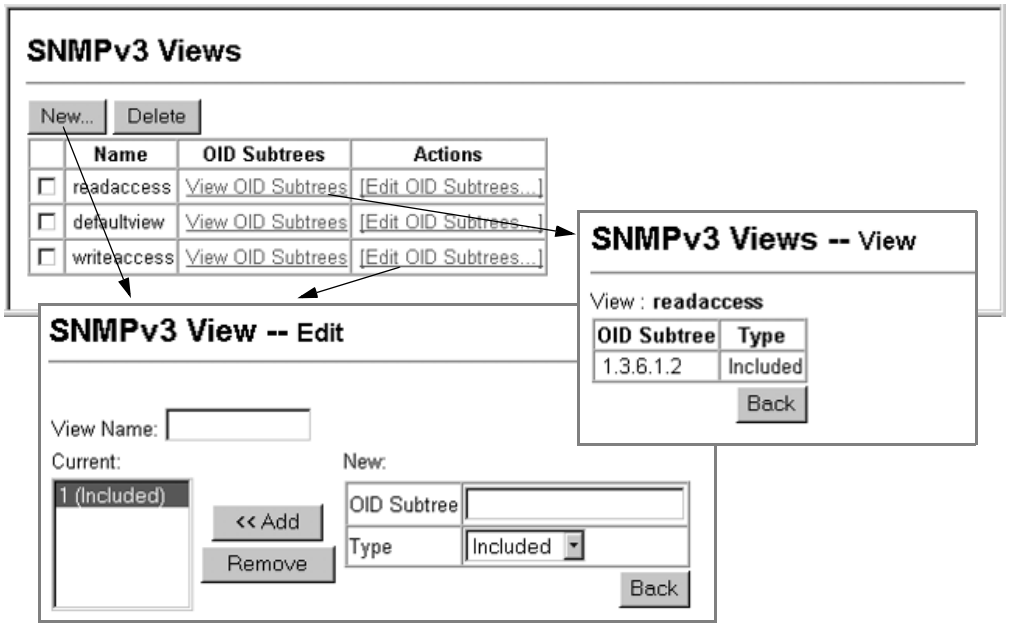
- **View Name** – The name of the SNMP view. (Range: 1-64 characters)
- **OID Subtree** – Specifies the initial object identifier of a branch within the MIB tree. Wild cards can be used to mask a specific portion of the OID string. Use the Add OID Subtree page to configure additional object identifiers.
- **Type** – Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view.

WEB INTERFACE

To configure an SNMP view of the switch's MIB database:

1. Click SNMP > SNMPv3 > Views.
2. Enter a view name and specify the initial OID subtree in the switch's MIB database to be included or excluded in the view. Use the Add OID Subtree page to add additional object identifier branches to the view.
3. Click Apply

Figure 46: Creating an SNMP View



6 SAMPLING TRAFFIC FLOWS

This chapter describes the following topics:

- sFlow Global Parameters – Enables sampling globally on the switch.
- sFlow Port Parameters – Sets the destination parameters for the sampled data, payload parameters, and sampling interval

OVERVIEW

The flow sampling (sFlow) feature embedded on this switch, together with a remote sFlow Collector, can provide network administrators with an accurate, detailed and real-time overview of the types and levels of traffic present on their network. The sFlow Agent samples 1 out of *n* packets from all data traversing the switch, re-encapsulates the samples as sFlow datagrams and transmits them to the sFlow Collector. This sampling occurs at the internal hardware level where all traffic is seen, whereas traditional probes will only have a partial view of traffic as it is sampled at the monitored interface. Moreover, the processor and memory load imposed by the sFlow agent is minimal since local analysis does not take place. The wire-speed transmission characteristic of the switch is thus preserved even at high traffic levels.

As the Collector receives streams from the various sFlow agents (other switches or routers) throughout the network, a timely, network-wide picture of utilization and traffic flows is created. Analysis of the sFlow stream(s) can reveal trends and information that can be leveraged in the following ways:

- Detecting, diagnosing, and fixing network problems
- Real-time congestion management
- Understanding application mix (P2P, Web, DNS, etc.) and changes
- Identification and tracing of unauthorized network activity
- Usage accounting
- Trending and capacity planning

CONFIGURING SFLOW GLOBAL PARAMETERS

Use the sFlow > Configuration page to enable sampling globally on the switch, as well as for those ports where it is required. Due to the switch's hardware design, flow sampling and the sampling rate can only be enabled for specific port groups as shown in the following table. However, sampling for each of the Gigabit ports (25-28/49-52) can be controlled individually.

CLI REFERENCES

- "Flow Sampling Commands" on page 545

PARAMETERS

These parameters are displayed:

- **Global Status** – Enables sFlow globally for the switch.
- **Group/Port Members** – The 100BASE-TX ports are organized into groups of 8 based on a restriction in the switch ASIC, and the 4 Gigabit ports each in it's own separate group.

Table 11: sFlow Groups and Port Members

Group	Level Group Port Members	
	ES3528M	ES3552M
1	1, 2, 3, 4, 5, 6, 7, 8	1, 2, 3, 4, 5, 6, 7, 8
2	9, 10, 11, 12, 13, 14, 15, 16	9, 10, 11, 12, 13, 14, 15, 16
3	17, 18, 19, 20, 21, 22, 23, 24	17, 18, 19, 20, 21, 22, 23, 24
4	25	25, 26, 27, 28, 29, 30, 31, 32
5	26	33, 34, 35, 36, 37, 38, 39, 40
6	27	41, 42, 43, 44, 45, 46, 47, 48
7	28	49
8		50
9		51
10		52

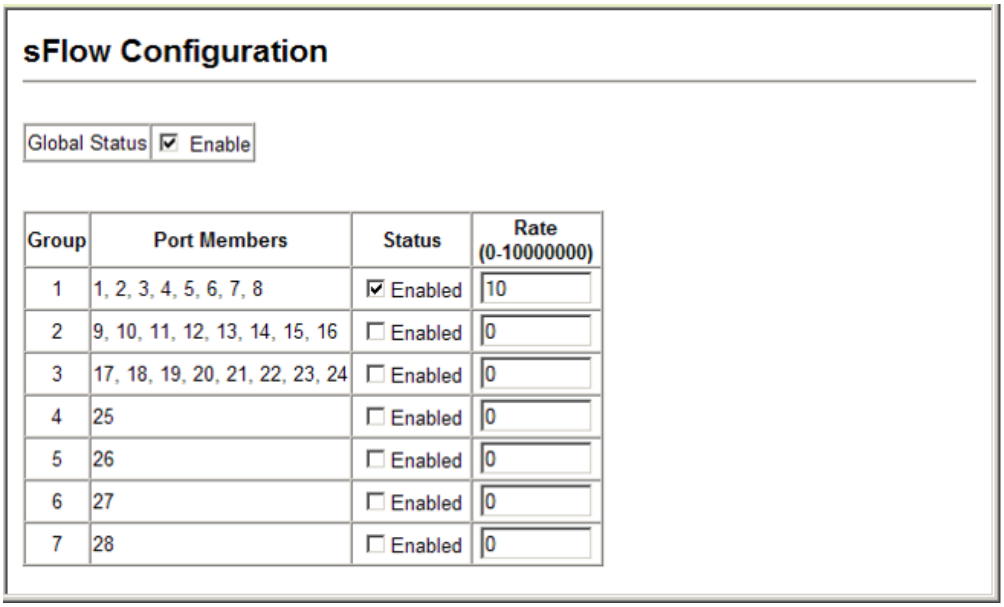
- **Status** – Enables sFlow on the ports in the indicated group.
- **Rate** – Configures the packet sampling rate. Setting the rate to 0 disables sampling. Setting the rate to 100 configures sampling to 1 packet out of every 100 received. (Range: 0-10000000; Default: 0)

WEB INTERFACE

To globally enable flow sampling:

1. Click sFlow, Configuration.
2. Set the global status for flow sampling, the ports or port groups to be sampled, and the sampling rate.
3. Click Apply

Figure 47: Configuring Global Settings for sFlow



CONFIGURING SFLOW PORT PARAMETERS

Use the sFlow > Port Configuration page to set the destination parameters for the sampled data, payload parameters, and sampling interval.

CLI REFERENCES

- "Flow Sampling Commands" on page 545

PARAMETERS

These parameters are displayed:

- **Port** – Choose the port to configure. (Range: 1-28/52; Default: 1)
- **Receiver Owner**[4] – The name of the receiver. (Range: 1-256 characters; Default: None)
- **Receiver IP Address**[4] – IP address of the sFlow Collector.

4. Sampling must be disabled by setting the time out to 0 before configuring these fields.

- **Receiver Port**[4] – The UDP port on which the sFlow Collector is listening for sFlow streams. (Range: 0-65534; Default: 6343)

- **Time Out** – The time that the sFlow process will continuously send samples to the Collector before resetting all sFlow port parameters (receiver owner, time out, max header size, max datagram size, and flow interval). A time out value of 0 seconds indicates no time out. (Range: 0-10000000 seconds; Default: 0 seconds)

  The check box is cleared by the system if flow sampling is currently under way. To change the timeout, mark the check box, enter a timeout value, and click Apply.

- **Max Header Size** – Maximum size of the sFlow datagram header. (Range: 64-256 bytes; Default: 128 bytes)

- **Max Datagram Size** – Maximum size of the sFlow datagram payload. (Range: 200-1500 bytes; Default: 1400 bytes)

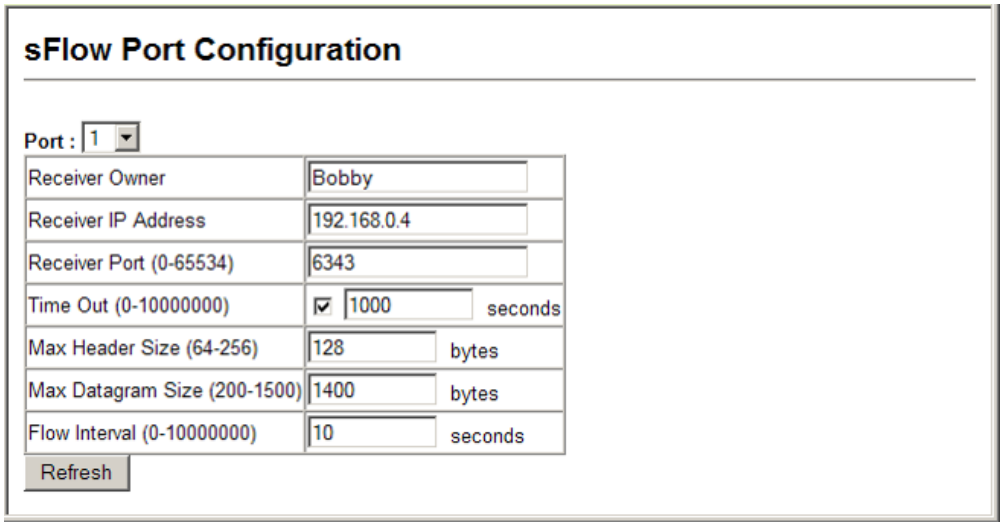
- **Flow Interval** – The interval at which the sFlow process adds counter values to the sample datagram. An interval of 0 seconds effectively disables this feature. (Range: 0-10000000 seconds; Default: 0 seconds)

WEB INTERFACE

To configure flow sampling on a port:

1. Click sFlow, Port Configuration.
2. Select a port to configure from the drop-down list.
3. Set the parameters for flow Collector, the reset timeout, the payload, and flow interval.
4. Click Apply

Figure 48: Configuring Global Settings for sFlow



7 SECURITY MEASURES

You can configure this switch to authenticate users logging into the system for management access using local or remote authentication methods. Port-based authentication using IEEE 802.1X can also be configured to control either management access to the uplink ports or client access to the data ports. This switch provides secure network management access using the following options:

- User Accounts – Manually configure access rights on the switch for specified users.
- Authentication Settings – Use remote authentication to configure access rights.
- Encryption Key – Configures RADIUS and TACACS+ encryption keys.
- AAA – Use local or remote authentication to configure access rights, specify authentication servers, configure remote authentication and accounting.
- HTTPS – Provide a secure web connection.
- SSH – Provide a secure shell (for secure Telnet access).
- Port Security – Configure secure addresses for individual ports.
- Port Authentication – Use IEEE 802.1X port authentication to control access to specific ports.
- Web Authentication – Allows stations to authenticate and access the network in situations where 802.1X or Network Access authentication methods are infeasible or impractical.
- Network Access - Configure MAC authentication, intrusion response, dynamic VLAN assignment, and dynamic QoS assignment.
- ACL – Access Control Lists provide packet filtering for IP frames (based on address, protocol, Layer 4 protocol port number or TCP control code).
- ARP Inspection – Security feature that validates the MAC Address bindings for Address Resolution Protocol packets. Provides protection against ARP traffic with invalid MAC to IP Address bindings, which forms the basis for certain "man-in-the-middle" attacks.
- IP Filter – Filters management access to the web, SNMP or Telnet interface.

- DHCP Snooping – Filter IP traffic on insecure ports for which the source address cannot be identified via DHCP snooping.
- IP Source Guard – Filters untrusted DHCP messages on insecure ports by building and maintaining a DHCP snooping binding table.

NOTE: The priority of execution for the filtering commands is Port Security, Port Authentication, Network Access, Web Authentication, Access Control Lists, IP Source Guard, and then DHCP Snooping.

CONFIGURING USER ACCOUNTS

Use the Security > User Accounts page to control management access to the switch based on manually configured user names and passwords.

CLI REFERENCES

- "User Accounts" on page 554

COMMAND USAGE

- The default guest name is "guest" with the password "guest." The default administrator name is "admin" with the password "admin."
- The guest only has read access for most configuration parameters. However, the administrator has write access for all parameters governing the onboard agent. You should therefore assign a new administrator password as soon as possible, and store it in a safe place.

PARAMETERS

These parameters are displayed:

- **User Name** – The name of the user.
  (Maximum length: 8 characters; maximum number of users: 16)
- **Access Level** – Specifies the user level. (Options: 0 - Normal, 8 - Manager, 15 - Privileged)

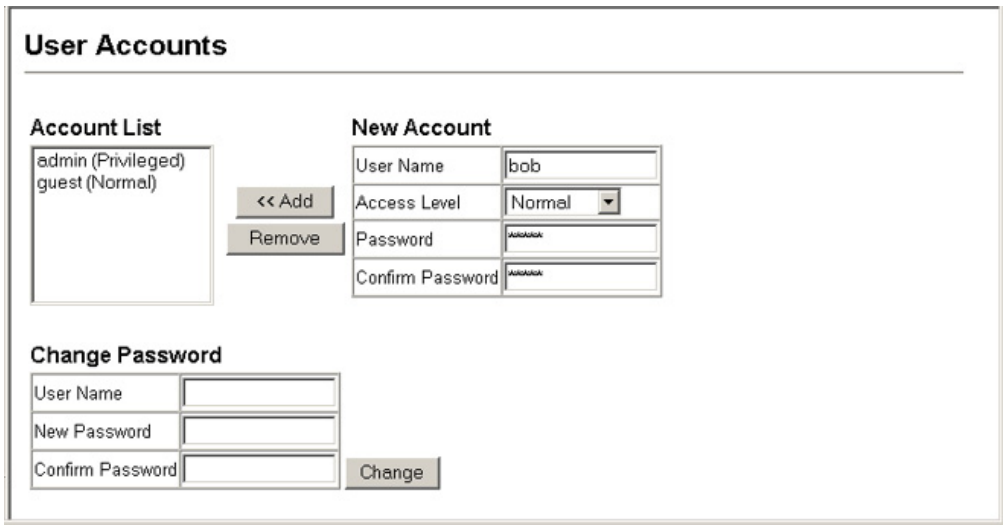
  Normal privilege level provides access to a limited number of the commands which display the current status of the switch, as well as several database clear and reset functions. Manager level provides access to all display status and configuration commands, except for those controlling various authentication and security features. Privileged level provides full access to all commands.
- **Password** – Specifies the user password.
  (Range: 0-8 characters plain text, case sensitive)
- **Confirm Password** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the password if these two fields do not match.

WEB INTERFACE

To configure user accounts:

1. Click Security, User Accounts.
2. Specify a user name, select the user's access level, then enter a password and confirm it.
3. Click Apply.

Figure 49: Configuring User Accounts



CONFIGURING LOCAL/REMOTE LOGON AUTHENTICATION

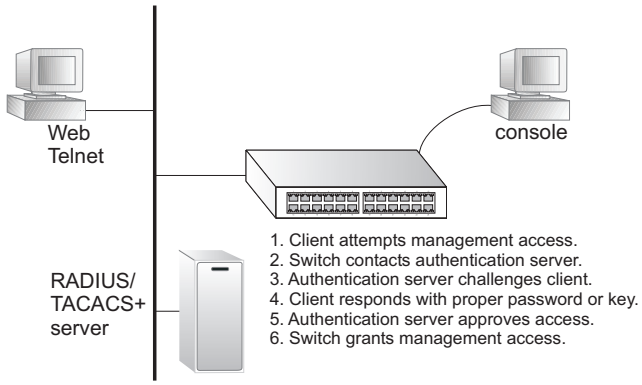
Use the Security > Authentication Settings menu to restrict management access based on specified user names and passwords. You can manually configure access rights on the switch, or you can use a remote access authentication server based on RADIUS or TACACS+ protocols.

CLI REFERENCES

- "Authentication Sequence" on page 556
- "RADIUS Client" on page 558
- "TACACS+ Client" on page 562

Remote Authentication Dial-in User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user that requires management access to the switch.

Figure 50: Authentication Server Operation



RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.

COMMAND USAGE

- By default, management access is always checked against the authentication database stored on the local switch. If a remote authentication server is used, you must specify the authentication sequence and the corresponding parameters for the remote authentication protocol. Local and remote logon authentication control management access via the console port, web browser, or Telnet.

- RADIUS and TACACS+ logon authentication assign a specific privilege level for each user name/password pair. The user name, password, and privilege level must be configured on the authentication server. The encryption methods used for the authentication process must also be configured or negotiated between the authentication server and logon client. This switch can pass authentication messages between the server and client that have been encrypted using MD5 (Message-Digest 5), TLS (Transport Layer Security), or TTLS (Tunneled Transport Layer Security).

- You can specify up to three authentication methods for any user to indicate the authentication sequence. For example, if you select (1) RADIUS, (2) TACACS and (3) Local, the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted using the TACACS+ server, and finally the local user name and password is checked.

PARAMETERS

These parameters are displayed:

- **Authentication Sequence** – Select the authentication, or authentication sequence required:

  - **Local** – User authentication is performed only locally by the switch.

- **RADIUS** – User authentication is performed using a RADIUS server only.
- **TACACS** – User authentication is performed using a TACACS+ server only.
- [authentication sequence] – User authentication is performed by up to three authentication methods in the indicated sequence.

◆ **RADIUS Settings**

- **Global** – Provides globally applicable RADIUS settings.
- **Server Index** – Specifies one of five RADIUS servers that may be configured. The switch attempts authentication using the listed sequence of servers. The process ends when a server either approves or denies access to a user.
- **Server IP Address** – Address of authentication server. (A Server Index entry must be selected to display this item.)
- **Authentication Port Number** – Network (UDP) port on authentication server used for authentication messages. (Range: 1-65535; Default: 1812)
- **Accounting Port Number** – Network (UDP) port on authentication server used for accounting messages. (Range: 1-65535; Default: 1813)
- **Number of Server Transmits** – Number of times the switch tries to authenticate logon access via the authentication server. (Range: 1-30; Default: 2)
- **Timeout for a Reply** – The number of seconds the switch waits for a reply from the RADIUS server before it resends the request. (Range: 1-65535; Default: 5)

◆ **TACACS Settings**

- **Global** – Provides globally applicable TACACS+ settings.
- **Server Index** – Specifies the index number of the server to be configured. The switch currently supports only one TACACS+ server.
- **Server IP Address** – Address of the TACACS+ server. (A Server Index entry must be selected to display this item.)
- **Server Port Number** – Network (TCP) port of TACACS+ server used for authentication messages. (Range: 1-65535; Default: 49)
- **Number of Server Transmits** – Number of times the switch tries to authenticate logon access via the authentication server. (Range: 1-30; Default: 2)

- **Timeout for a Reply** – The number of seconds the switch waits for a reply from the RADIUS server before it resends the request. (Range: 1-540; Default: 5)

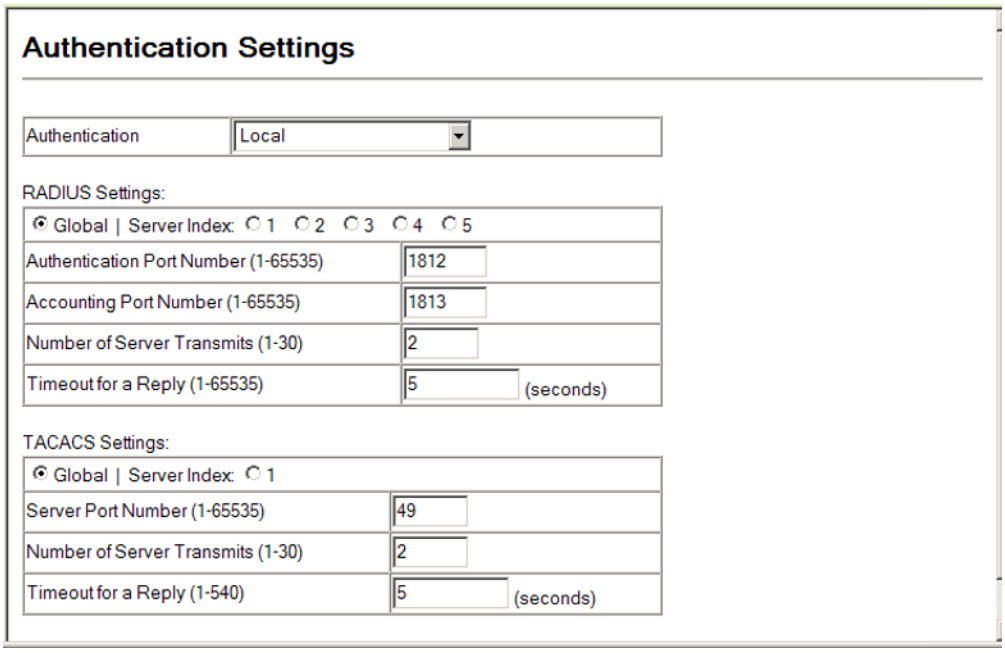
NOTE: The local switch user database has to be set up by manually entering user names and passwords (see "Configuring User Accounts.")

WEB INTERFACE

To configure the method(s) of controlling management access:

1. Click Security, Authentication Settings.
2. Specify the authentication sequence (i.e., one to three methods), and fill in the parameters for RADIUS or TACACS+ authentication if selected.
3. Click Apply.

Figure 51: Configuring Authentication Settings



CONFIGURING ENCRYPTION KEYS

Use the Security > Encryption Key page to configure encryption keys for all RADIUS and TACACS+ servers.

CLI REFERENCES

- "RADIUS Client" on page 558
- "TACACS+ Client" on page 562

PARAMETERS

These parameters are displayed:

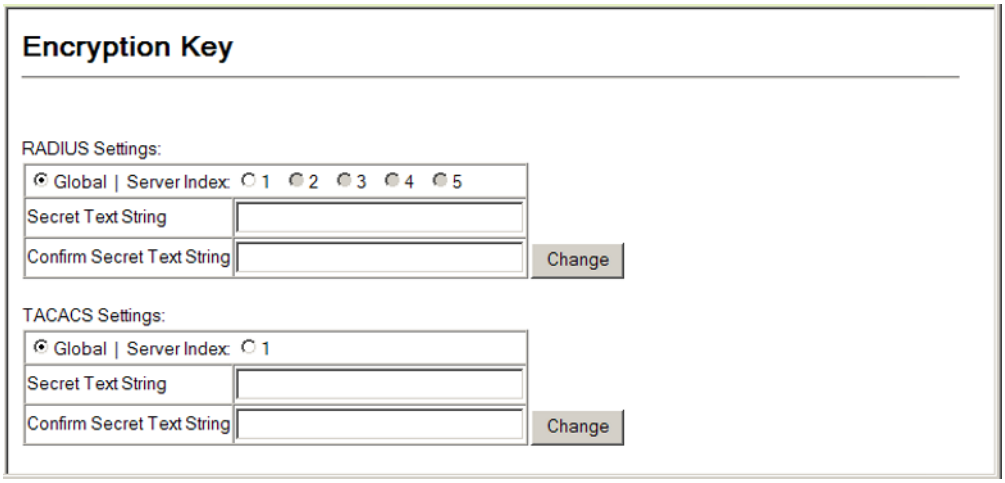
- **RADIUS Settings**
  - **Global** – Provides globally applicable RADIUS encryption key settings.
  - **Server Index** – Specifies one of five RADIUS servers for which an encryption key may be configured.
  - **Secret Text String** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)
  - **Confirm Secret Text String** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the encryption key if these two fields do not match.
- **TACACS Settings**
  - **Global** – Provides globally applicable TACACS+ encryption key settings.
  - **ServerIndex** – Specifies the index number of the TACACS+ server for which an encryption key may be configured. The switch currently supports only one TACACS+ server.
  - Secret Text String – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)
  - Confirm Secret Text String – Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the encryption key if these two fields do not match.

WEB INTERFACE

To configure encryption keys:

1. Click Security, Encryption Key.
2. Choose the appropriate RADIUS or TACACS+ Server Index, enter Secret Text String and confirm it.
3. Click Change.

Figure 52: Configuring Encryption Keys



AAA AUTHORIZATION AND ACCOUNTING

The Authentication, authorization, and accounting (AAA) feature provides the main framework for configuring access control on the switch. The three security functions can be summarized as follows:

- Authentication — Identifies users that request access to the network.
- Authorization — Determines if users can access specific services.
- Accounting — Provides reports, auditing, and billing for services that users have accessed on the network.

The AAA functions require the use of configured RADIUS or TACACS+ servers in the network. The security servers can be defined as sequential groups that are applied as a method for controlling user access to specified services. For example, when the switch attempts to authenticate a user, a request is sent to the first server in the defined group, if there is no response the second server will be tried, and so on. If at any point a pass or fail is returned, the process stops.

The switch supports the following AAA features:

- Accounting for IEEE 802.1X authenticated users that access the network through the switch.
- Accounting for users that access management interfaces on the switch through the console and Telnet.
- Accounting for commands that users enter at specific CLI privilege levels.
- Authorization of users that access management interfaces on the switch through the console and Telnet.

To configure AAA on the switch, you need to follow this general process:

1. Configure RADIUS and TACACS+ server access parameters. See "Configuring Local/Remote Logon Authentication."
2. Define RADIUS and TACACS+ server groups to support the accounting and authorization of services.
3. Define a method name for each service to which you want to apply accounting or authorization and specify the RADIUS or TACACS+ server groups to use.
4. Apply the method names to port or line interfaces.

NOTE: This guide assumes that RADIUS and TACACS+ servers have already been configured to support AAA. The configuration of RADIUS and TACACS+ server software is beyond the scope of this guide, refer to the documentation provided with the RADIUS or TACACS+ server software.

CONFIGURING AAA RADIUS GROUP SETTINGS

Use the AAA > RADIUS Group Settings screen to define the configured RADIUS servers to use for accounting and authorization.

CLI REFERENCES

- "AAA" on page 566

PARAMETERS

These parameters are displayed:

- **Group Name** - Defines a name for the RADIUS server group. (1-255 characters)
- **Server Index** - Specifies the RADIUS server and sequence to use for the group. (Range: 1-5)

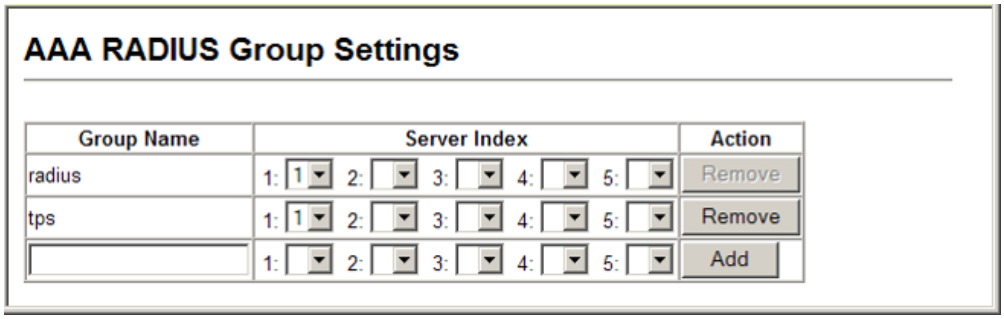
  When specifying the index for a RADIUS sever, the server index must already be defined (see "Configuring Local/Remote Logon Authentication").

WEB INTERFACE

To configure the RADIUS server groups to use for accounting and authorization:

1. Click Security, AAA, RADIUS Group Settings.
2. Enter the group name, and select the index of the server to use for each priority level.
3. Click Add.

Figure 53: Configuring AAA RADIUS Server Groups



CONFIGURING AAA TACACS+ GROUP SETTINGS

Use the AAA > TACACS+ Group Settings screen to define the configured TACACS+ servers to use for accounting and authorization.

CLI REFERENCES

- "AAA" on page 566

PARAMETERS

These parameters are displayed:

- **Group Name** - Defines a name for the TACACS+ server group. (1-255 characters)
- **Server** - Specifies the TACACS+ server to use for the group. (Range: 1)

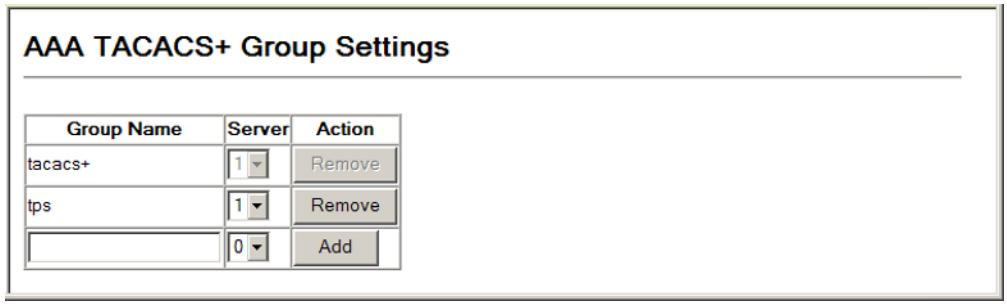
  When specifying the index for a TACACS+ sever, the server index must already be defined (see "Configuring Local/Remote Logon Authentication").

WEB INTERFACE

To configure the TACACS+ server groups to use for accounting and authorization:

1. Click Security, AAA, TACACS+ Group Settings.
2. Enter the group name, followed by the number of the server.
3. Click Add.

Figure 54: Configuring AAA TACACS+ Server Groups



CONFIGURING AAA ACCOUNTING SETTINGS

Use the Security > AAA > Accounting > Settings page to enable accounting of requested services for billing or security purposes.

CLI REFERENCES

- "AAA" on page 566

COMMAND USAGE

AAA authentication through a RADIUS or TACACS+ server must be enabled before accounting is enabled.

PARAMETERS

These parameters are displayed:

- **Method Name** – Specifies an accounting method for service requests. The "default" methods are used for a requested service if no other methods have been defined. (Range: 1-255 characters)

  Note that the method name is only used to describe the accounting method configured on the specified RADIUS or TACACS+ servers. No information is sent to the servers about the method to use.

- **Service Request** – Specifies the service as:

  - **802.1X** – Accounting for end users.
  - **Exec** – Administrative accounting for local console, Telnet, or SSH connections.
  - **Commands** – Administrative accounting to apply to commands entered at specific CLI privilege levels.

- **Accounting Notice** – Records user activity from log-in to log-off point.

- **Group Name** - Specifies the accounting server group. (Range: 1-255 characters)

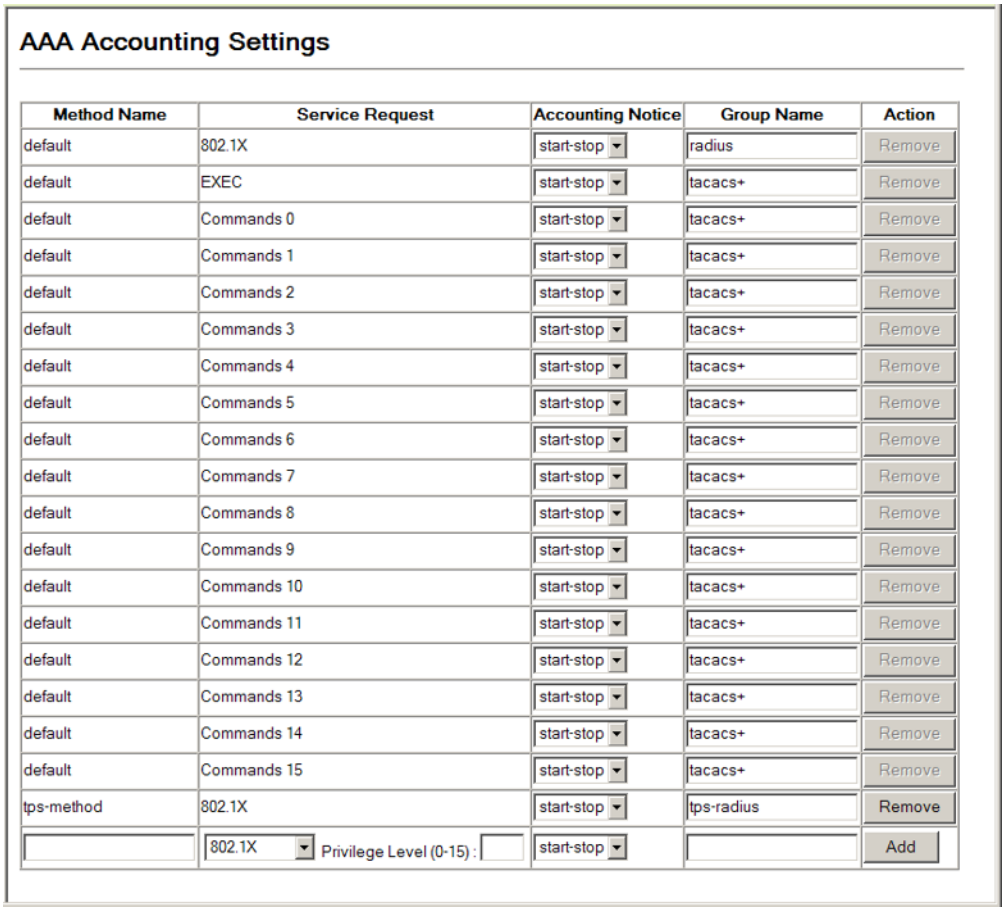
  The group names "radius" and "tacacs+" specifies all configured RADIUS and TACACS+ hosts (see "Configuring Local/Remote Logon Authentication"). Any other group name refers to a server group configured on the RADIUS or TACACS+ Group Settings pages.

WEB INTERFACE

To configure the accounting method applied to various service types and the assigned server group:

1. Click Security, AAA, Accounting, Settings.
2. Specify a method name, the type of service request, and a group name.
3. Click Add.

Figure 55: Configuring the Methods Used for AAA Accounting



CONFIGURING AAA ACCOUNTING UPDATE TIME

Use the Security > AAA > Accounting > Periodic Update page to set the interval at which accounting updates are sent to accounting servers.

CLI REFERENCES

- "aaa accounting update" on page 570

PARAMETERS

These parameters are displayed:

- **Periodic Update** - Specifies the interval at which the local accounting service updates information for all users on the system to the accounting server. (Range: 0-2147483647 minutes; where 0 means disabled; Default: 1 minute)

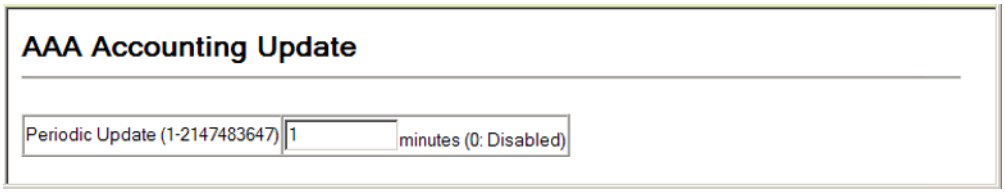
WEB INTERFACE

To configure update interval for AAA accounting:

1. Click Security, AAA, Accounting, Periodic Update.
2. Enter the required update interval.

3. Click Apply.

Figure 56: Configuring the Update Interval for AAA Accounting



AAA ACCOUNTING 802.1X PORT SETTINGS

Use the Security > AAA > Accounting > 802.1X Port Settings page to specify the accounting method applied to an interface.

CLI REFERENCES

- "accounting dot1x" on page 572

PARAMETERS

These parameters are displayed:

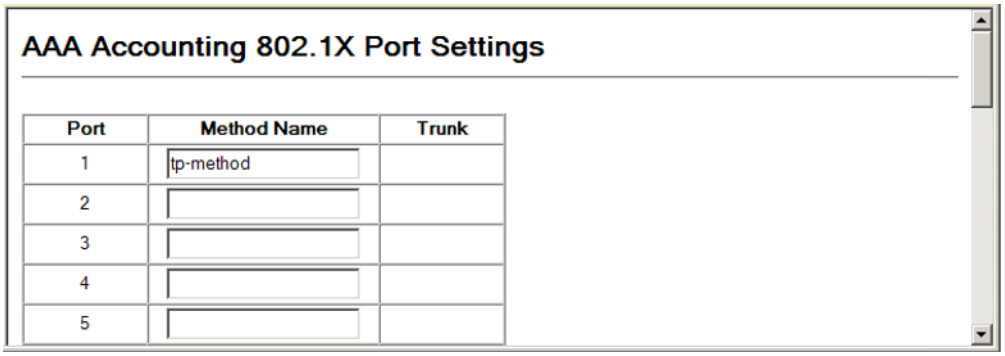
- **Port/Trunk** - Specifies a port or trunk number.
- **Method Name** – Specifies a user defined accounting method to apply to an interface. This method must be defined in the Configure Method page. (Range: 1-255 characters)

WEB INTERFACE

To configure the accounting method applied to specific interfaces:

1. Click Security, AAA, Accounting, 802.1X Port Settings.
2. Enter the required accounting method.
3. Click Apply.

Figure 57: Configuring 802.1X Port Settings for the Accounting Method



CONFIGURING AAA ACCOUNTING EXEC COMMAND PRIVILEGES

Use the Security > AAA > Accounting > Command Privileges page to specify a method name to apply to commands entered at specific CLI privilege levels.

CLI REFERENCES

- "accounting commands" on page 573

PARAMETERS

These parameters are displayed:

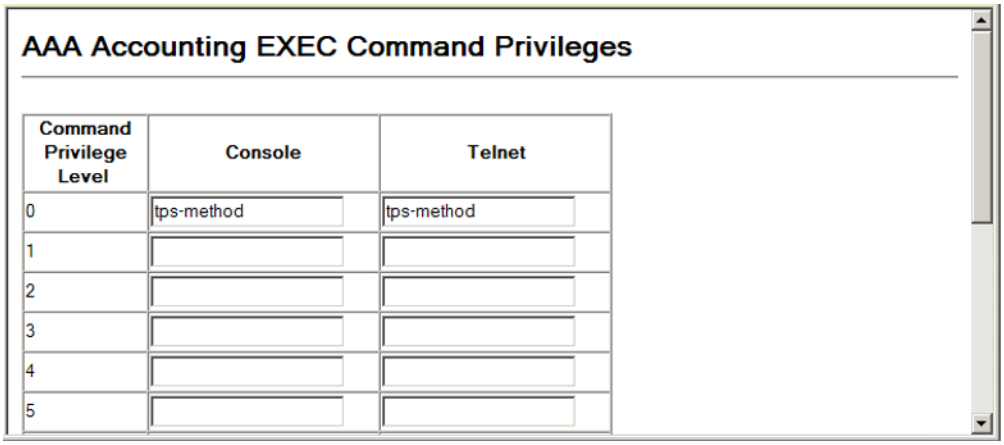
- **Commands Privilege Level** – The CLI privilege levels (0-15).
- **Console** – Specifies a user-defined method name to apply to commands entered at the specified CLI privilege level through the console interface.
- **Telnet** – Specifies a user-defined method name to apply to commands entered at the specified CLI privilege level through Telnet.

WEB INTERFACE

To configure the accounting method applied to specific CLI privilege levels:

1. Click Security, AAA, Accounting, Command Privileges.
2. Enter a defined method name for console and Telnet privilege levels.
3. Click Apply.

Figure 58: Configuring AAA Accounting Service for CLI Privilege Levels



CONFIGURING AAA ACCOUNTING EXEC SETTINGS

Use the Security > AAA > Accounting > Exec Settings page to specify a method name to apply to console and Telnet connections.

CLI REFERENCES

- "accounting exec" on page 573

PARAMETERS

These parameters are displayed:

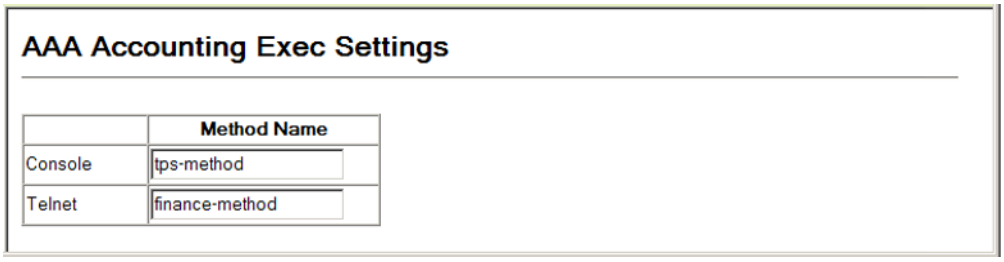
- **Console** – Specifies a user defined method name to apply to console connections.
- **Telnet** – Specifies a user defined method name to apply to Telnet connections.

WEB INTERFACE

To configure the accounting method applied to console and Telnet connections:

1. Click Security, AAA, Accounting, Exec Settings.
2. Enter a defined method name for console and Telnet connections
3. Click Apply.

Figure 59: Configuring AAA Accounting Service for Exec Service



DISPLAYING THE AAA ACCOUNTING SUMMARY

Use the Security > AAA > Accounting > Summary page to display all the configured accounting methods, the methods applied to specified management interfaces, and basic accounting information recorded for user sessions.

CLI REFERENCES

- "show accounting" on page 575

PARAMETERS

These parameters are displayed:

Summary

- **Accounting Type** - Displays the accounting service.
- **Method List** - Displays the user-defined or default accounting method.

- **Group List** - Displays the accounting server group.
- **Interface** - Displays the port, console or Telnet interface to which these rules apply. (This field is null if the accounting method and associated server group has not been assigned to an interface.)

Statistics

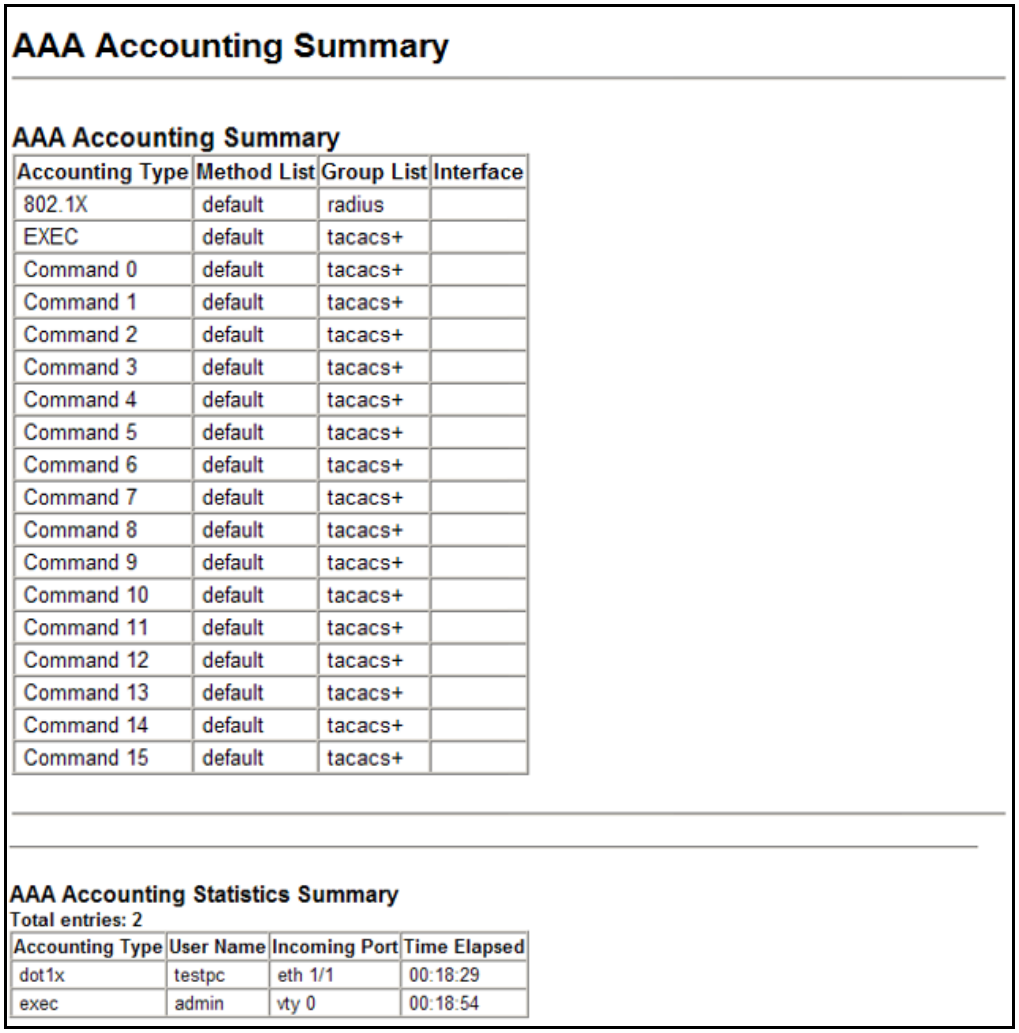
- **Accounting Type** - Displays the accounting service.
- **User Name** - Displays a registered user name.
- **Interface** - Displays the receive port number through which this user accessed the switch.
- **Time Elapsed** - Displays the length of time this entry has been active.

WEB INTERFACE

To display a summary of the configured accounting methods and assigned server groups for specified service types, and statistics recorded for user sessions:

1. Click Security, AAA, Accounting, Summary.

Figure 60: Displaying a Summary of Applied AAA Accounting Methods



AAA Accounting Summary

AAA Accounting Summary

Accounting Type	Method List	Group List	Interface
802.1X	default	radius	
EXEC	default	tacacs+	
Command 0	default	tacacs+	
Command 1	default	tacacs+	
Command 2	default	tacacs+	
Command 3	default	tacacs+	
Command 4	default	tacacs+	
Command 5	default	tacacs+	
Command 6	default	tacacs+	
Command 7	default	tacacs+	
Command 8	default	tacacs+	
Command 9	default	tacacs+	
Command 10	default	tacacs+	
Command 11	default	tacacs+	
Command 12	default	tacacs+	
Command 13	default	tacacs+	
Command 14	default	tacacs+	
Command 15	default	tacacs+	

AAA Accounting Statistics Summary

Total entries: 2

Accounting Type	User Name	Incoming Port	Time Elapsed
dot1x	testpc	eth 1/1	00:18:29
exec	admin	vty 0	00:18:54

CONFIGURING AUTHORIZATION SETTINGS

Use the Security > AAA > Authorization page to configure the authorization method used for requested services.

CLI REFERENCES

- "aaa authorization exec" on page 570

COMMAND USAGE

- This feature performs authorization to determine if a user is allowed to run an Exec shell.
- AAA authentication through a RADIUS or TACACS+ server must be enabled before authorization is enabled.

PARAMETERS

These parameters are displayed:

- **Method Name** – Specifies an authorization method for service requests. The "default" method is used for a requested service if no other methods have been defined. (Range: 1-255 characters)
- **Service Request** – Specifies the service as Exec (administrative authorization for local console, Telnet, or SSH connections) or Commands.
- **Group Name** - Specifies the authorization server group. (Range: 1-255 characters)

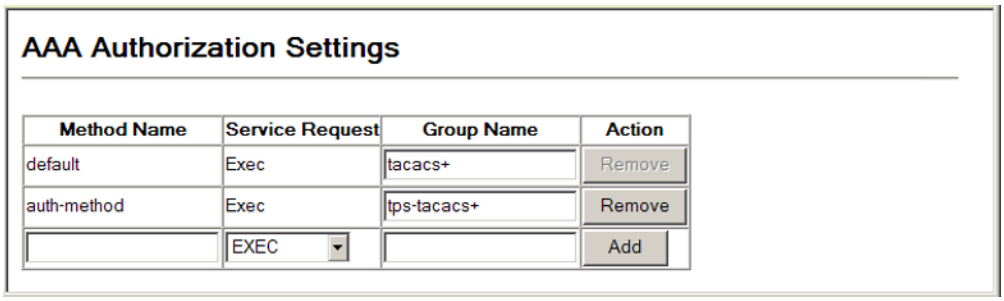
  The group name "tacacs+" specifies all configured TACACS+ hosts (see "Configuring Local/Remote Logon Authentication"). Any other group name refers to a server group configured on the TACACS+ Group Settings page. Authorization is only supported for TACACS+ servers.

WEB INTERFACE

To configure the authorization method applied to the Exec service type and the assigned server group:

1. Click Security, AAA, Authorization, Settings.
2. Specify the name of the authorization method and server group name.
3. Click Add.

Figure 61: Configuring AAA Authorization Methods



CONFIGURING AUTHORIZATION EXEC SETTINGS

Use the Security > AAA > Authorization > Exec Settings page to specify the authorization method applied to console and Telnet connections.

CLI REFERENCES

- "aaa authorization exec" on page 570

PARAMETERS

These parameters are displayed:

- **Console** – Specifies a user defined method name to apply to console connections.

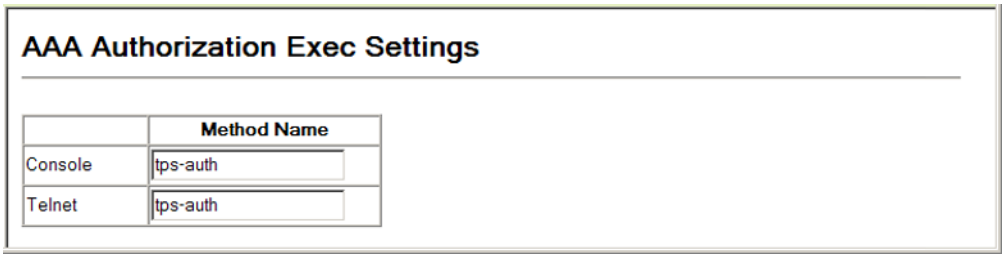
- **Telnet** – Specifies a user defined method name to apply to Telnet connections. (Note that Telnet includes SSH connections.)

WEB INTERFACE

To configure the authorization method applied to local console and Telnet connections:

1. Click Security, AAA, Authorization, Exec Settings.
2. Enter the required authorization method for console and Telnet connections.
3. Click Apply.

Figure 62: Configuring AAA Authorization Methods for Exec Service



AUTHORIZATION SUMMARY

Use the Security > AAA > Authorization > Summary page to display the configured authorization methods and the interfaces to which they are applied.

CLI REFERENCES

- "show accounting" on page 575

PARAMETERS

These parameters are displayed:

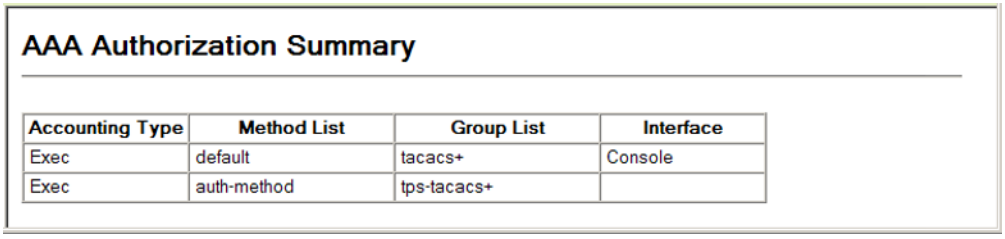
- **Authorization Type** - Displays the authorization service.
- **Method Name** - Displays the user-defined or default accounting method.
- **Group List** - Displays the authorization server group.
- **Interface** - Displays the console or Telnet interface to which these rules apply. (This field is null if the authorization method and associated server group has not been assigned to an interface.)

WEB INTERFACE

To display a the configured authorization method and assigned server groups for the Exec service type:

1. Click Security, AAA, Authorization, Summary.

Figure 63: Displaying the Applied AAA Authorization Method



CONFIGURING HTTPS

You can configure the switch to enable the Secure Hypertext Transfer Protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's web interface.

CONFIGURING GLOBAL SETTINGS FOR HTTPS

Use the Security > HTTPS Settings page to enable or disable HTTPS and specify the UDP port used for this service.

CLI REFERENCES

- "Web Server" on page 576

COMMAND USAGE

- Both the HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure both services to use the same UDP port. (HTTP can only be configured through the CLI using the ip http server command.)
- If you enable HTTPS, you must indicate this in the URL that you specify in your browser: https://*device*[:*port_number*]
- When you start HTTPS, the connection is established in this way:
  - The client authenticates the server using the server's digital certificate.
  - The client and server negotiate a set of security protocols to use for the connection.
  - The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection.

  A padlock icon should appear in the status bar for Internet Explorer 5.x or above, Netscape 6.2 or above, and Mozilla Firefox 2.0.0.0 or above.

- The following web browsers and operating systems currently support HTTPS:

Table 12: HTTPS System Support

Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Windows Vista, Windows 7
Netscape 6.2 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6
Mozilla Firefox 2.0.0.0 or later	Windows 2000, Windows XP, Linux

- To specify a secure-site certificate, see "Replacing the Default Secure-site Certificate".

PARAMETERS

These parameters are displayed:

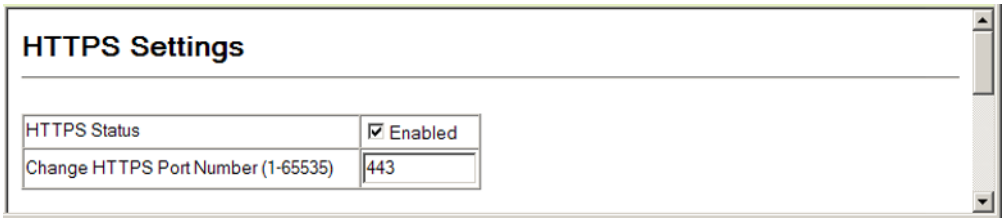
- **HTTPS Status** – Allows you to enable/disable the HTTPS server feature on the switch. (Default: Enabled)
- **Change HTTPS Port Number** – Specifies the UDP port number used for HTTPS connection to the switch's web interface. (Default: Port 443)

WEB INTERFACE

To configure HTTPS:

1. Click Security, HTTPS Settings.
2. Enable HTTPS and specify the port number if required.
3. Click Apply.

Figure 64: Configuring HTTPS



REPLACING THE DEFAULT SECURE-SITE CERTIFICATE

Use the Security > HTTPS Settings page to replace the default secure-site certificate.

When you log onto the web interface using HTTPS (for secure access), a Secure Sockets Layer (SSL) certificate appears for the switch. By default, the certificate that Netscape and Internet Explorer display will be associated with a warning that the site is not recognized as a secure site. This is because the certificate has not been signed by an approved certification authority. If you want this warning to be replaced by a

message confirming that the connection to the switch is secure, you must obtain a unique certificate and a private key and password from a recognized certification authority.

CAUTION: For maximum security, we recommend you obtain a unique Secure Sockets Layer certificate at the earliest opportunity. This is because the default certificate for the switch is not unique to the hardware you have purchased.

When you have obtained these, place them on your TFTP server and transfer them to the switch to replace the default (unrecognized) certificate with an authorized one.

NOTE: The switch must be reset for the new certificate to be activated. To reset the switch, see "Resetting the System."

CLI REFERENCES

- "Web Server" on page 576

PARAMETERS

These parameters are displayed:

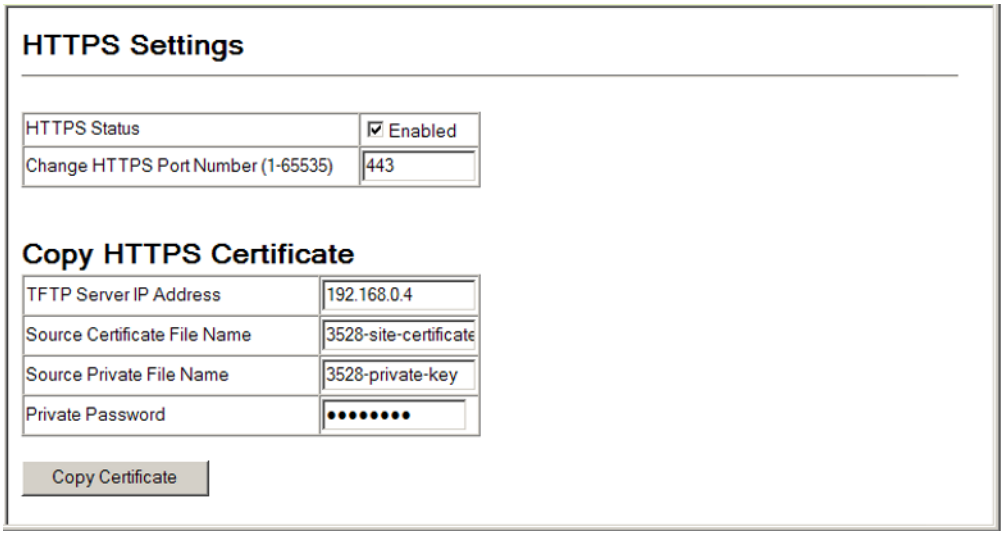
- **TFTP Server IP Address** – IP address of TFTP server which contains the certificate file.
- **Source Certificate File Name** – Name of certificate file stored on the TFTP server.
- **Source Private File Name** – Name of private key file stored on the TFTP server.
- **Private Password** – Password stored in the private key file. This password is used to verify authorization for certificate use, and is verified when downloading the certificate to the switch.

WEB INTERFACE

To replace the default secure-site certificate:

1. Click Security, HTTPS Settings.
2. Fill in the TFTP server, certificate and private key file name, and private password.
3. Click Copy Certificate.

Figure 65: Downloading the Secure-Site Certificate



CONFIGURING THE SECURE SHELL

The Berkeley-standard includes remote access tools originally designed for Unix systems. Some of these tools have also been implemented for Microsoft Windows and other environments. These tools, including commands such as *rlogin* (remote login), *rsh* (remote shell), and *rcp* (remote copy), are not secure from hostile attacks.

The Secure Shell (SSH) includes server/client applications intended as a secure replacement for the older Berkeley remote access tools. SSH can also provide remote management access to this switch as a secure replacement for Telnet. When the client contacts the switch via the SSH protocol, the switch generates a public-key that the client uses along with a local user name and password for access authentication. SSH also encrypts all data transfers passing between the switch and SSH-enabled management station clients, and ensures that data traveling over the network arrives unaltered.

NOTE: You need to install an SSH client on the management station to access the switch for management via the SSH protocol.

NOTE: The switch supports both SSH Version 1.5 and 2.0 clients.

COMMAND USAGE

The SSH server on this switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified on the Authentication Settings page (page 171). If public key authentication is specified by the client, then you must configure authentication keys on both the client and the switch as described in the following section. Note that regardless of

whether you use public key or password authentication, you still have to generate authentication keys on the switch (SSH Host Key Settings) and enable the SSH server (Authentication Settings).

To use the SSH server, complete these steps:

1. *Generate a Host Key Pair* – On the SSH Host Key Settings page, create a host public/private key pair.

2. *Provide Host Public Key to Clients* – Many SSH client programs automatically import the host public key during the initial connection setup with the switch. Otherwise, you need to manually create a known hosts file on the management station and place the host public key in it. An entry for a public key in the known hosts file would appear similar to the following example:

   10.1.0.54 1024 35
   156849954018676692593339467750546173253136748908365472541502024559319986854435836165199992332978176606583095610825913212890233 765468017262725714134287629413011961955667825956641048695742788814620651941746772984865468615717739390164779355942303577413098022737087794545240839717526463580581767167095748047761117

3. *Import Client's Public Key to the Switch* – See "Importing User Public Keys," or use the copy tftp public-key command (page 473) to copy a file containing the public key for all the SSH client's granted management access to the switch. (Note that these clients must be configured locally on the switch via the User Accounts page as described on page 170.) The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as shown in the following example for an RSA Version 1 key:

   1024 35
   134108168560989392104094492015542534763164192187295892114317388005553616163105177594083868631109291232226828519254374603100937187721199696317813662774141689851320491172048303392543241016379975923714490119380060902539484084827178194372288402533115952134861022902978982721353267131629432532818915045306393916643steve@192.168.1.19

4. *Set the Optional Parameters* – On the SSH Settings page, configure the optional parameters, including the authentication timeout, the number of retries, and the server key size.

5. *Enable SSH Service* – On the SSH Settings page, enable the SSH server on the switch.

6. Authentication – One of the following authentication methods is employed:

   Password Authentication (for SSH v1.5 or V2 Clients)

   a. The client sends its password to the server.
   b. The switch compares the client's password to those stored in memory.

c. If a match is found, the connection is allowed.

NOTE: To use SSH with only password authentication, the host public key must still be given to the client, either during initial connection or manually entered into the known host file. However, you do not need to configure the client's keys.

Public Key Authentication – When an SSH client attempts to contact the switch, the SSH server uses the host key pair to negotiate a session key and encryption method. Only clients that have a private key corresponding to the public keys stored on the switch can access it. The following exchanges take place during this process:

Authenticating SSH v1.5 Clients

a. The client sends its RSA public key to the switch.
b. The switch compares the client's public key to those stored in memory.
c. If a match is found, the switch uses its secret key to generate a random 256-bit string as a challenge, encrypts this string with the user's public key, and sends it to the client.
d. The client uses its private key to decrypt the challenge string, computes the MD5 checksum, and sends the checksum back to the switch.
e. The switch compares the checksum sent from the client against that computed for the original string it sent. If the two checksums match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

Authenticating SSH v2 Clients

a. The client first queries the switch to determine if DSA public key authentication using a preferred algorithm is acceptable.
b. If the specified algorithm is supported by the switch, it notifies the client to proceed with the authentication process. Otherwise, it rejects the request.
c. The client sends a signature generated using the private key to the switch.
d. When the server receives this message, it checks whether the supplied key is acceptable for authentication, and if so, it then checks whether the signature is correct. If both checks succeed, the client is authenticated.

NOTE: The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.

CONFIGURING THE SSH SERVER

Use the Security > SSH (Configure Global) page to enable the SSH server and configure basic settings for authentication.

NOTE: A host key pair must be configured on the switch before you can enable the SSH server. See "Generating the Host Key Pair."

CLI REFERENCES

- "Secure Shell" on page 580

PARAMETERS

These parameters are displayed:

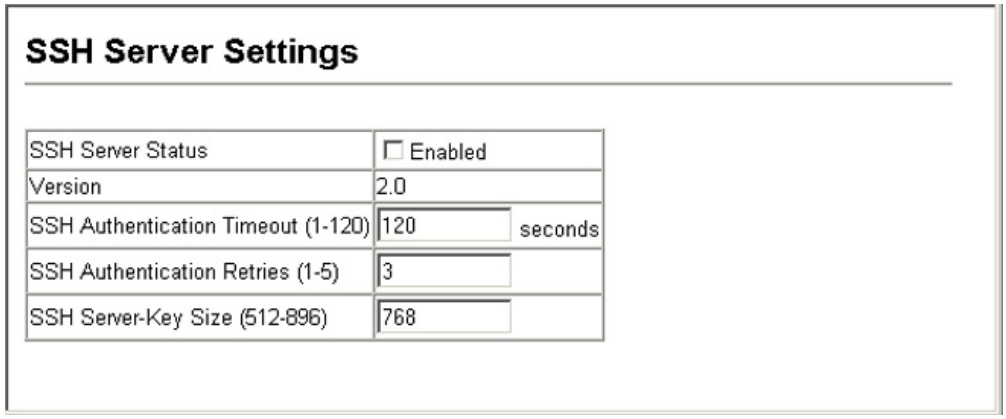
- **SSH Server Status** – Allows you to enable/disable the SSH server on the switch. (Default: Disabled)
- **Version** – The Secure Shell version number. Version 2.0 is displayed, but the switch supports management access via either SSH Version 1.5 or 2.0 clients.
- **SSH Authentication Timeout** – Specifies the time interval in seconds that the SSH server waits for a response from a client during an authentication attempt. (Range: 1-120 seconds; Default: 120 seconds)
- **SSH Authentication Retries** – Specifies the number of authentication attempts that a client is allowed before authentication fails and the client has to restart the authentication process. (Range: 1-5 times; Default: 3)
- **SSH Server-Key Size** – Specifies the SSH server key size. (Range: 512-896 bits; Default:768)
  - The server key is a private key that is never shared outside the switch.
  - The host key is shared with the SSH client, and is fixed at 1024 bits.

WEB INTERFACE

To configure the SSH server:

1. Click Security, SSH, Settings.
2. Enable the SSH server.
3. Adjust the authentication parameters as required.
4. Click Apply.

Figure 66: Configuring the SSH Server



GENERATING THE HOST KEY PAIR

Use the Security > SSH > Host-Key Settings page to generate a host public/private key pair used to provide secure communications between an SSH client and the switch. After generating this key pair, you must provide the host public key to SSH clients and import the client's public key to the switch as described in the section "Importing User Public Keys."

NOTE: A host key pair must be configured on the switch before you can enable the SSH server. See "Configuring the SSH Server."

CLI REFERENCES

- "Secure Shell" on page 580

PARAMETERS

These parameters are displayed:

- **Public-Key of Host-Key** – The public key for the host.
  - RSA (Version 1): The first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 65537), and the last string is the encoded modulus.
  - DSA (Version 2): The first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS). The last string is the encoded modulus.
- **Host-Key Type** – The key type used to generate the host key pair (i.e., public and private keys). (Range: RSA (Version 1), DSA (Version 2), Both; Default: Both)

  The SSH server uses RSA or DSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.

NOTE: The switch uses only RSA Version 1 for SSHv1.5 clients and DSA Version 2 for SSHv2 clients.

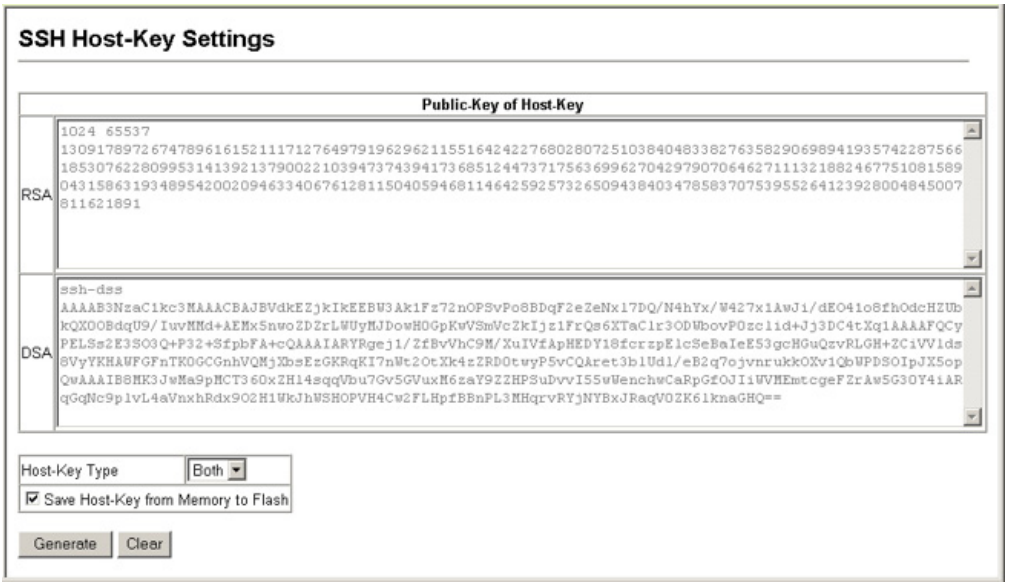
- **Save Host-Key from Memory to Flash** – Saves the host key from RAM (i.e., volatile memory) to flash memory. Otherwise, the host key pair is stored to RAM by default. Note that you must select this item prior to generating the host-key pair. (Default: Disabled)
- **Generate** – This button is used to generate the host key pair. Note that you must first generate the host key pair before you can enable the SSH server on the SSH Server Settings page.
- **Clear** – This button clears the host key from both volatile memory (RAM) and non-volatile memory (Flash).

WEB INTERFACE

To generate the SSH host key pair:

1. Click Security, SSH, Host-Key Settings.
2. Select the host-key type from the drop-down box.
3. Select the option to save the host key from memory to flash if required.
4. Click Generate.

Figure 67: Generating the SSH Host Key Pair



IMPORTING USER PUBLIC KEYS

Use the Security > SSH > User Public-Key Settings page to upload a user's public key to the switch. This public key must be stored on the switch for the user to be able to log in using the public key authentication mechanism. If the user's public key does not exist on the switch, SSH will revert to the interactive password authentication mechanism to complete authentication.

CLI REFERENCES

- "Secure Shell" on page 580

PARAMETERS

These parameters are displayed:

- **Public-Key of** *user* – The RSA and DSA public keys for the selected user.
  - RSA: The first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 37), and the last string is the encoded modulus.
  - DSA: The first field indicates that SSH version 2 was used to create the key. The second field contains the key comment. The third string is the encoded modulus, and the last field is a comment denoting the end of the key.
- **User Name** – This drop-down box selects the user who's public key you wish to manage. Note that you must first create users on the User Accounts page (see "Configuring User Accounts").
- **Public-Key Type** – The type of public key to upload.
  - RSA: The switch accepts a RSA version 1 encrypted public key.
  - DSA: The switch accepts a DSA version 2 encrypted public key.

  The SSH server uses RSA or DSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.

  The switch uses only RSA Version 1 for SSHv1.5 clients and DSA Version 2 for SSHv2 clients.
- **TFTP Server IP Address** – The IP address of the TFTP server that contains the public key file you wish to import.
- **Source File Name** – The public key file to upload.
- **Copy Public Key** – Initiates the public key TFTP import process. If you are replacing an outdated public key file, it is not necessary to first delete the original key from the switch. The import process will overwrite the existing key.

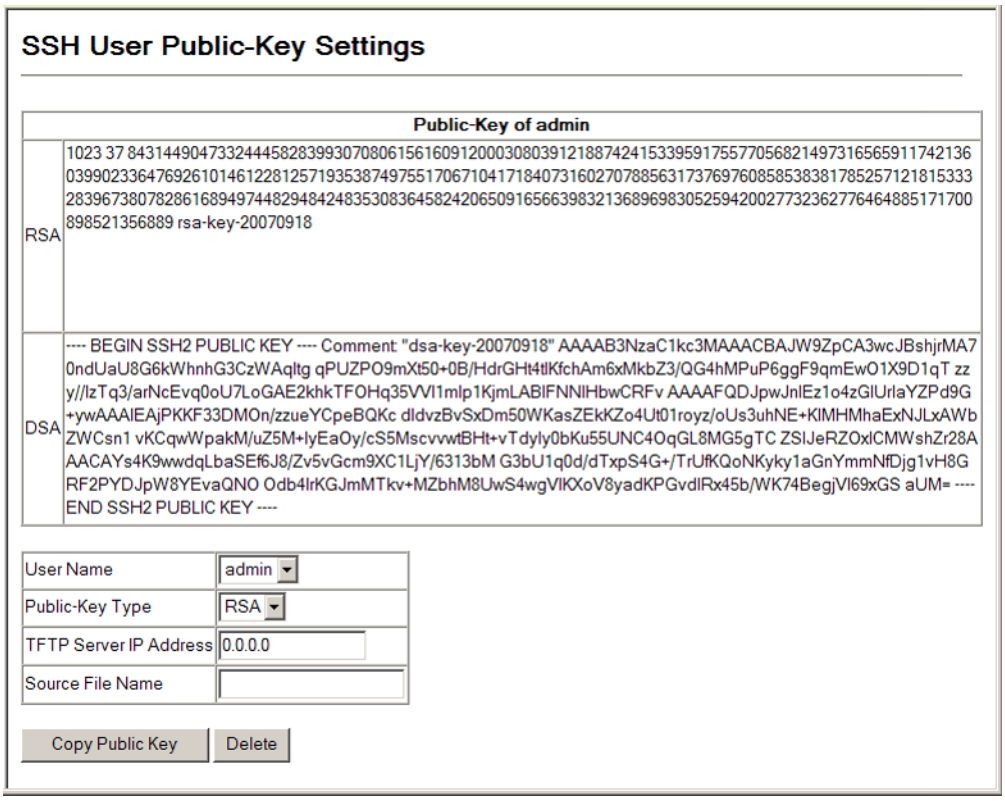
- **Delete** – Deletes a selected RSA or DSA public key that has already been imported to the switch.

WEB INTERFACE

To copy the SSH user's public key:

1. Click Security, SSH, User Public-Key Settings.
2. Select the user name and the public-key type from the respective drop-down boxes, input the TFTP server IP address and the public key source file name.
3. Set your browser to allow pop-ups.
4. Click Copy Public Key.

Figure 68: Copying the SSH User's Public Key



CONFIGURING PORT SECURITY

Use the Security > Port Security page to configure a switch port with one or more device MAC addresses that are authorized to access the network through that port.

When port security is enabled on a port, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum

number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be authorized to access the network through that port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

To use port security, specify a maximum number of addresses to allow on the port and then let the switch dynamically learn the <source MAC address, VLAN> pair for frames received on the port. Note that you can also manually add secure addresses to the port using the Static Address Table (page 293). When the port has reached the maximum number of MAC addresses, the selected port will stop learning. The MAC addresses already in the address table will be retained and will not age out. Any other device that attempts to use the port will be prevented from accessing the switch.

CLI REFERENCES

- "Port Security" on page 614

COMMAND USAGE

- A secure port has the following restrictions:
  - It cannot be used as a member of a static or dynamic trunk.
  - It should not be connected to a network interconnection device.
- The default maximum number of MAC addresses allowed on a secure port is zero. You must configure a maximum address count from 1 - 1024 for the port to allow access.
- If a port is disabled (shut down) due to a security violation, it must be manually re-enabled from the Port > Port Configuration page (page 261).

PARAMETERS

These parameters are displayed:

- **Port** – Port number.
- **Name** – Descriptive text (page 262).
- **Action** – Indicates the action to be taken when a port security violation is detected:
  - **None**: No action should be taken. (This is the default.)
  - **Trap**: Send an SNMP trap message.
  - **Shutdown**: Disable the port.
  - **Trap and Shutdown**: Send an SNMP trap message and disable the port.

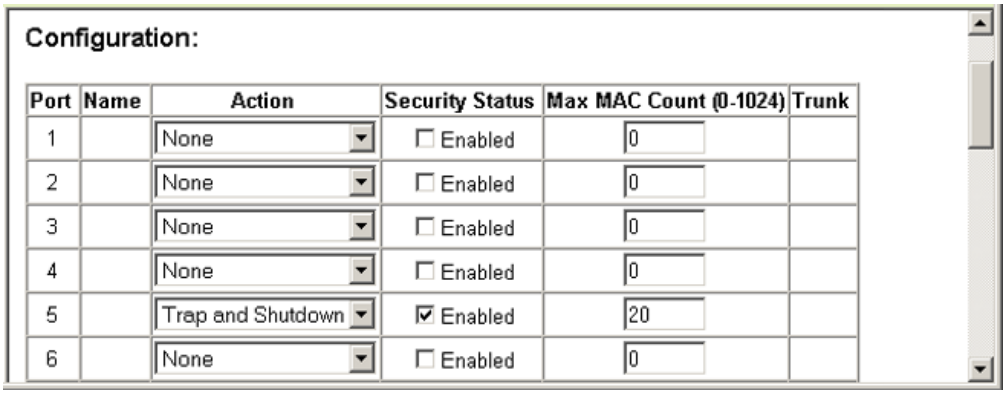
- **Security Status** – Enables or disables port security on the port. (Default: Disabled)
- **Max MAC Count** – The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 1024, where 0 means disabled)
- **Trunk** – Trunk number if port is a member.

WEB INTERFACE

To configure port security:

1. Click Security, Port Security.
2. Set the action to take when an invalid address is detected on a port, mark the check box in the Security Status column to enable security for a port, and set the maximum number of MAC addresses allowed on a port.
3. Click Apply

Figure 69: Configuring Port Security



CONFIGURING 802.1X PORT AUTHENTICATION

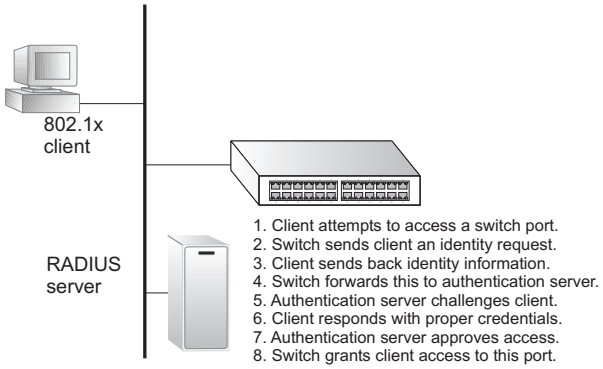
Network switches can provide open and easy access to network resources by simply attaching a client PC. Although this automatic configuration and access is a desirable feature, it also allows unauthorized personnel to easily intrude and possibly gain access to sensitive network data.

The IEEE 802.1X (dot1X) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. Access to all switch ports in a network can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

This switch uses the Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol messages with the client, and a remote RADIUS authentication server to verify user identity and access

rights. When a client (i.e., Supplicant) connects to a switch port, the switch (i.e., Authenticator) responds with an EAPOL identity request. The client provides its identity (such as a user name) in an EAPOL response to the switch, which it forwards to the RADIUS server. The RADIUS server verifies the client identity and sends an access challenge back to the client. The EAP packet from the RADIUS server contains not only the challenge, but the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. The encryption method used to pass authentication messages can be MD5 (Message-Digest 5), TLS (Transport Layer Security), PEAP (Protected Extensible Authentication Protocol), or TTLS (Tunneled Transport Layer Security). The client responds to the appropriate method with its credentials, such as a password or certificate. The RADIUS server verifies the client credentials and responds with an accept or reject packet. If authentication is successful, the switch allows the client to access the network. Otherwise, non-EAP traffic on the port is blocked or assigned to a guest VLAN based on the "intrusion-action" setting. In "multi-host" mode, only one host connected to a port needs to pass authentication for all other hosts to be granted network access. Similarly, a port can become unauthorized for all hosts if one attached host fails re-authentication or sends an EAPOL logoff message.

Figure 70: Configuring Port Security



The operation of 802.1X on the switch requires the following:

- The switch must have an IP address assigned.
- RADIUS authentication must be enabled on the switch and the IP address of the RADIUS server specified.
- 802.1X must be enabled globally for the switch.
- Each switch port that will be used must be set to dot1X "Auto" mode.
- Each client that needs to be authenticated must have dot1X client software installed and properly configured.
- The RADIUS server and 802.1X client support EAP. (The switch only supports EAPOL in order to pass the EAP packets from the server to the client.)

- The RADIUS server and client also have to support the same EAP authentication type – MD5, PEAP, TLS, or TTLS. (Native support for these encryption methods is provided in Windows XP, and in Windows 2000 with Service Pack 4. To support these encryption methods in Windows 95 and 98, you can use the AEGIS dot1x client or other comparable client software)

DISPLAYING 802.1X GLOBAL SETTINGS

Use the Security > 802.1X > Information page to display the global setting for IEEE 802.1X port authentication and EAPOL pass through.

CLI REFERENCES

- "802.1X Port Authentication" on page 590

PARAMETERS

These parameters are displayed:

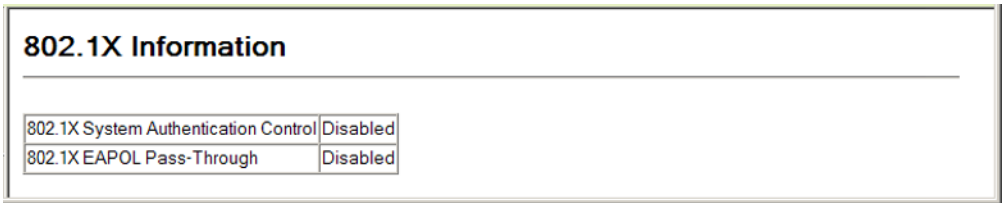
- **802.1X System Authentication Control** – The global setting for 802.1X.
- **EAPOL Pass Through** – When enabled, this feature passes EAPOL frames through to all ports in STP forwarding state when dot1x is globally disabled.

WEB INTERFACE

To show the global settings for 802.1X:

1. Click Security, 802.1X, Information.

Figure 71: Displaying Global Settings for 802.1X Port Authentication



CONFIGURING 802.1X GLOBAL SETTINGS

Use the Security > 802.1X > Configuration page to configure IEEE 802.1X port authentication. The 802.1X protocol must be enabled globally for the switch system before port settings are active.

CLI REFERENCES

- "802.1X Port Authentication" on page 590

PARAMETERS

These parameters are displayed:

- **Port Authentication Status** – Sets the global setting for 802.1X. (Default: Disabled)

- **EAPOL Pass Through** – Passes EAPOL frames through to all ports in STP forwarding state when dot1x is globally disabled. (Default: Disabled)

  When this device is functioning as intermediate node in the network and does not need to perform dot1x authentication, **EAPOL Pass Through** can be enabled to allow the switch to forward EAPOL frames from other switches on to the authentication servers, thereby allowing the authentication process to still be carried out by switches located on the edge of the network.

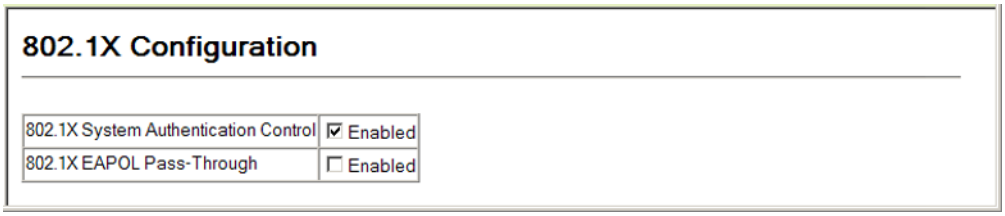
  When this device is functioning as an edge switch but does not require any attached clients to be authenticated, **EAPOL Pass Through** can be disabled to discard unnecessary EAPOL traffic.

WEB INTERFACE

To configure global settings for 802.1X:

1. Click Security, 802.1X, Configuration.
2. Enable 802.1X globally for the switch, and configure EAPOL Pass Through if required.
3. Click Apply

Figure 72: Configuring Global Settings for 802.1X Port Authentication



CONFIGURING AUTHENTICATOR PORT SETTINGS FOR 802.1X

Use the Security > 802.1X > Authenticator Port Configuration page to configure 802.1X port settings for the switch as the local authenticator. When 802.1X is enabled, you need to configure the parameters for the authentication process that runs between the client and the switch (i.e., authenticator), as well as the client identity lookup process that runs between the switch and authentication server.

CLI REFERENCES

- "802.1X Port Authentication" on page 590

PARAMETERS

These parameters are displayed:

- **Port** – Port number.
- **Status** – Indicates if authentication is enabled or disabled on the port. The status is disabled if the control mode is set to Force-Authorized.

- **Operation Mode** – Allows single or multiple hosts (clients) to connect to an 802.1X-authorized port. (Default: Single-Host)
  - **Single-Host** – Allows only a single host to connect to this port.
  - **Multi-Host** – Allows multiple host to connect to this port.

    In this mode, only one host connected to a port needs to pass authentication for all other hosts to be granted network access. Similarly, a port can become unauthorized for all hosts if one attached host fails re-authentication or sends an EAPOL logoff message.
  - **MAC-Based** – Allows multiple hosts to connect to this port, with each host needing to be authenticated.

    In this mode, each host connected to a port needs to pass authentication. The number of hosts allowed access to a port operating in this mode is limited only by the available space in the secure address table (i.e., up to 1024 addresses).
- **Max MAC Count** – The maximum number of hosts that can connect to a port when the Multi-Host operation mode is selected. (Range: 1-1024; Default: 5)
- **Mode** – Sets the authentication mode to one of the following options:
  - **Auto** – Requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.
  - **Force-Authorized** – Forces the port to grant access to all clients, either dot1x-aware or otherwise. (This is the default setting.)
  - **Force-Unauthorized** – Forces the port to deny access to all clients, either dot1x-aware or otherwise.
- **Re-authentication** – Sets the client to be re-authenticated after the interval specified by the Re-authentication Period. Re-authentication can be used to detect if a new device is plugged into a switch port. (Default: Disabled)
- **Max-Request** – Sets the maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session. (Range: 1-10; Default 2)
- **Quiet Period** – Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client. (Range: 1-65535 seconds; Default: 60 seconds)
- **Re-authentication Period** – Sets the time period after which a connected client must be re-authenticated. (Range: 1-65535 seconds; Default: 3600 seconds)

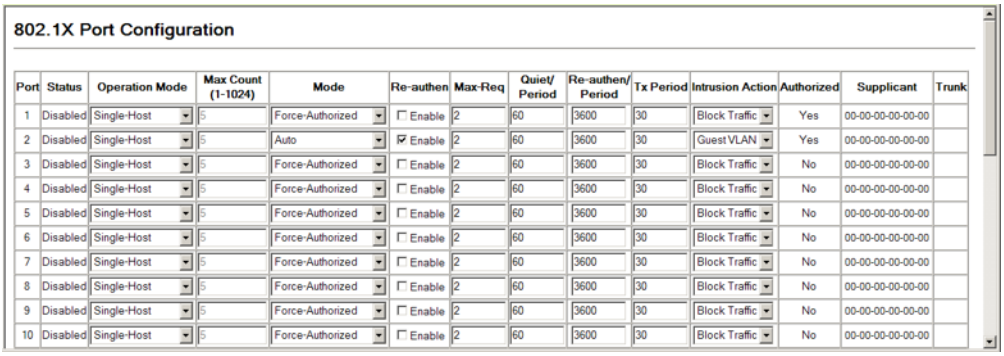
- **Tx Period** – Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet. (Range: 1-65535; Default: 30 seconds)
- **Intrusion Action** – Sets the port's response to a failed authentication.
  - **Block Traffic** – Blocks all non-EAP traffic on the port. (This is the default setting.)
  - **Guest VLAN** – All traffic for the port is assigned to a guest VLAN. The guest VLAN must be separately configured (See "Configuring VLAN Groups") and mapped on each port (See "Configuring Network Access for Ports").
- **Authorized** – Displays the 802.1X authorization status of connected clients.
  - **Yes** – Connected client is authorized.
  - **No** – Connected client is not authorized.
- **Supplicant** – Indicates the MAC address of a connected client.
- **Trunk** – Indicates if the port is configured as a trunk port.

WEB INTERFACE

To configure port authenticator settings for 802.1X:

1. Click Security, 802.1X, Authenticator Port Configuration.
2. Modify the authentication settings for each port as required.
3. Click Apply

Figure 73: Configuring Interface Settings for 802.1X Port Authenticator



CONFIGURING SUPPLICANT PORT SETTINGS FOR 802.1X

Use the Security > 802.1X > Supplicant Port Configuration page to configure 802.1X port settings for supplicant requests issued from a port to an authenticator on another device. When 802.1X is enabled and the control mode is set to Force-Authorized (see "Configuring Authenticator Port Settings for 802.1X" on page 203), you need to configure the parameters for the client supplicant process if the client must be authenticated through another device in the network.

CLI REFERENCES

- "802.1X Port Authentication" on page 605

COMMAND USAGE

- When devices attached to a port must submit requests to another authenticator on the network, configure the Identity Profile parameters which identify this switch as a supplicant, and configure the supplicant parameters for those ports which must authenticate clients through the remote authenticator on this configuration page. When PAE supplicant mode is enabled on a port, it will not respond to dot1x messages meant for an authenticator.

- This switch can be configured to serve as the authenticator on selected ports by setting the Control Mode to Auto on the Authenticator Port configuration page, and as a supplicant on other ports by the setting the control mode to Force-Authorized on that configuration page and enabling the PAE supplicant on the Supplicant Port configuration page.

PARAMETERS

These parameters are displayed in the web interface:

Global Settings

- **Identity Profile User Name** – The dot1x supplicant user name. (Range: 1-8 characters)

  The global supplicant user name and password are used to identify this switch as a supplicant when responding to an MD5 challenge from the authenticator. These parameters must be set when this switch passes client authentication requests to another authenticator on the network.

- **Identity Profile Password** – The dot1x supplicant password used to identify this switch as a supplicant when responding to an MD5 challenge from the authenticator. (Range: 1-8 characters)

Port Settings

- **Port** – Port number.

- **PAE Supplicant** – Enables PAE supplicant mode. (Default: Disabled)

  If the attached client must be authenticated through another device in the network, supplicant status must be enabled.

  Supplicant status can only be enabled if PAE Control Mode is set to "Force-Authorized" on this port (see "Configuring Authenticator Port Settings for 802.1X" on page 203).

PAE supplicant status cannot be enabled if a port is a member of trunk or LACP is enabled on the port.

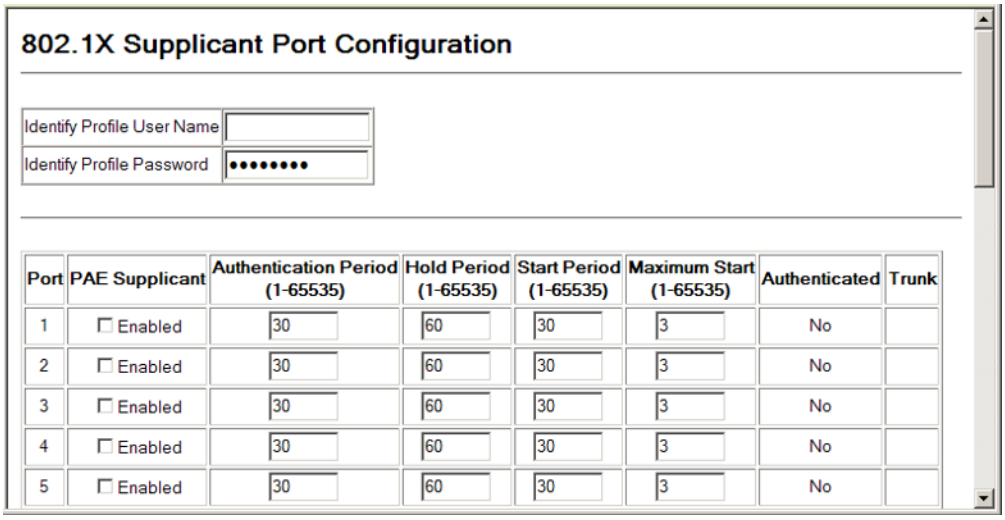
- **Authentication Period** – The time that a supplicant port waits for a response from the authenticator. (Range: 1-65535 seconds; Default: 30 seconds)
- **Hold Period** – The time that a supplicant port waits before resending its credentials to find a new an authenticator. (Range: 1-65535 seconds; Default: 30 seconds)
- **Start Period** – The time that a supplicant port waits before resending an EAPOL start frame to the authenticator. (Range: 1-65535 seconds; Default: 30 seconds)
- **Maximum Start** – The maximum number of times that a port supplicant will send an EAP start frame to the client before assuming that the client is 802.1X unaware. (Range: 1-65535; Default: 3)
- **Authenticated** – Shows whether or not the supplicant has been authenticated.

WEB INTERFACE

To configure port supplicant settings for 802.1X:

1. Click Security, 802.1X, Supplicant Port Configuration.
2. Then set the identity user name and password to use when the switch responds an MD5 challenge from the authentication server.
3. Modify the supplicant settings for each port as required.
4. Click Apply

Figure 74: Configuring Interface Settings for 802.1X Port Supplicant



DISPLAYING 802.1X AUTHENTICATOR STATISTICS

Use the Security > 802.1X > Authenticator Statistics page to display statistics for dot1x authenticator exchanges for any port.

CLI REFERENCES

- "show dot1x" on page 601

PARAMETERS

These parameters are displayed:

Table 13: 802.1X Authenticator Statistics

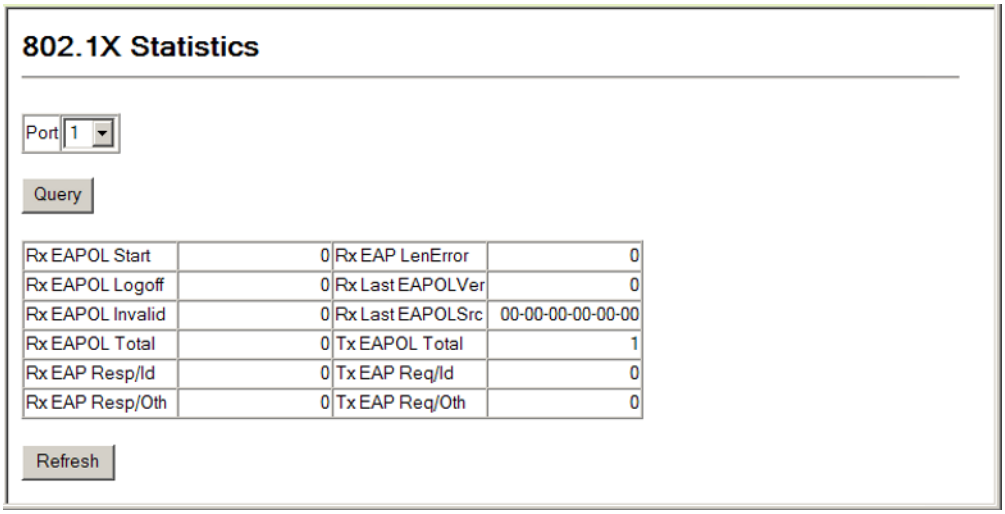
Parameter	Description
Rx EAPOL Start	The number of EAPOL Start frames that have been received by this Authenticator.
Rx EAPOL Logoff	The number of EAPOL Logoff frames that have been received by this Authenticator.
Rx EAPOL Invalid	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
Rx EAPOL Total	The number of valid EAPOL frames of any type that have been received by this Authenticator.
Rx Last EAPOLVer	The protocol version number carried in the most recent EAPOL frame received by this Authenticator.
Rx Last EAPOLSrc	The source MAC address carried in the most recent EAPOL frame received by this Authenticator.
Rx EAP Resp/Id	The number of EAP Resp/Id frames that have been received by this Authenticator.
Rx EAP Resp/Oth	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
Rx EAP LenError	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
Tx EAP Req/Id	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
Tx EAP Req/Oth	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.
Tx EAPOL Total	The number of EAPOL frames of any type that have been transmitted by this Authenticator.

WEB INTERFACE

To display port authenticator statistics for 802.1X:

1. Click Security, 802.1X > Authenticator Statistics.
2. Select a port from the scroll-down list.
3. Click Query.

Figure 75: Showing Statistics for 802.1X Port Authenticator



DISPLAYING 802.1X SUPPLICANT STATISTICS

Use the Security > 802.1X > Supplicant Statistics page to display statistics for dot1x supplicant exchanges for any port.

CLI REFERENCES

- "show dot1x" on page 601

PARAMETERS

These parameters are displayed:

Table 14: 802.1X Supplicant Statistics

Parameter	Description
Rx EAPOL Invalid	The number of EAPOL frames that have been received by this Supplicant in which the frame type is not recognized.
Rx EAPOL Total	The number of valid EAPOL frames of any type that have been received by this Supplicant.
Rx EAP Resp/Id	The number of EAP Resp/Id frames that have been received by this Supplicant.
Rx EAP Resp/Oth	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Supplicant.
Rx EAP LenError	The number of EAPOL frames that have been received by this Supplicant in which the Packet Body Length field is invalid.
Rx Last EAPOLVer	The protocol version number carried in the most recent EAPOL frame received by this Supplicant.

Table 14: 802.1X Supplicant Statistics (Continued)

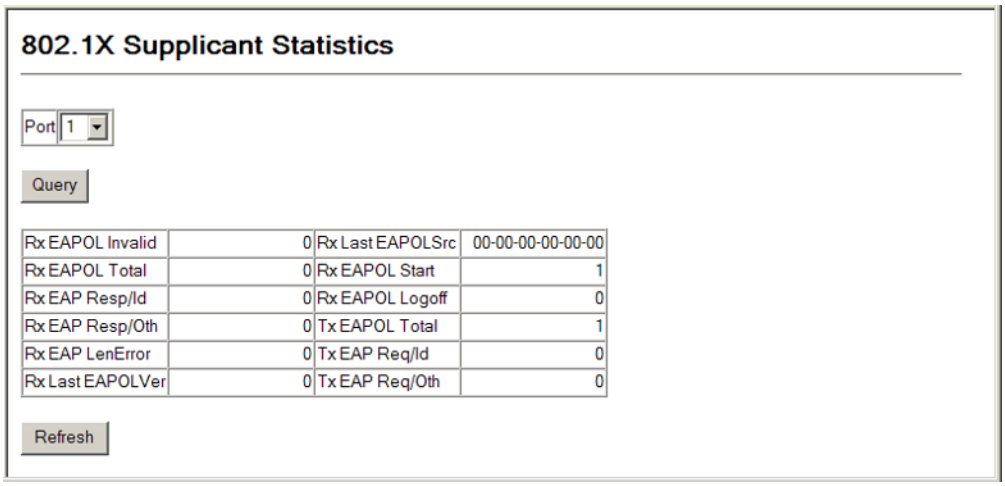
Parameter	Description
Rx Last EAPOLSrc	The source MAC address carried in the most recent EAPOL frame received by this Supplicant.
Rx EAPOL Start	The number of EAPOL Start frames that have been received by this Supplicant.
Rx EAPOL Logoff	The number of EAPOL Logoff frames that have been received by this Supplicant.
Tx EAPOL Total	The number of EAPOL frames of any type that have been transmitted by this Supplicant.
Tx EAP Req/Id	The number of EAP Req/Id frames that have been transmitted by this Supplicant.
Tx EAP Req/Oth	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Supplicant.

WEB INTERFACE

To display port supplicant statistics for 802.1X:

1. Click Security, 802.1X > Supplicant Statistics.
2. Select a port from the scroll-down list.
3. Click Query.

Figure 76: Showing Statistics for 802.1X Port Supplicant



WEB AUTHENTICATION

Web authentication allows stations to authenticate and access the network in situations where 802.1X or Network Access authentication are infeasible or impractical. The web authentication feature allows unauthenticated hosts to request and receive a DHCP assigned IP address and perform DNS queries. All other traffic, except for HTTP protocol traffic, is blocked. The

switch intercepts HTTP protocol traffic and redirects it to a switch-generated web page that facilitates user name and password authentication via RADIUS. Once authentication is successful, the web browser is forwarded on to the originally requested web page. Successful authentication is valid for all hosts connected to the port.

NOTE: RADIUS authentication must be activated and configured properly for the web authentication feature to work properly. (See "Configuring Local/Remote Logon Authentication.")

NOTE: Web authentication cannot be configured on trunk ports.

CONFIGURING GLOBAL SETTINGS FOR WEB AUTHENTICATION

Use the Security > Web Authentication > Configuration page to edit the global parameters for web authentication.

CLI REFERENCES

- "Web Authentication" on page 629

PARAMETERS

These parameters are displayed:

- **System Authentication Control** – Enables web authentication for the switch. (Default: Disabled)

  Note that this feature must also be enabled for any port where required under the Configure Interface menu.

- **Session Timeout** – Configures how long an authenticated session stays active before it must re-authenticate itself. (Range: 300-3600 seconds; Default: 3600 seconds)

- **Quiet Period** – Configures how long a host must wait to attempt authentication again after it has exceeded the maximum allowable failed login attempts. (Range: 1-180 seconds; Default: 60 seconds)

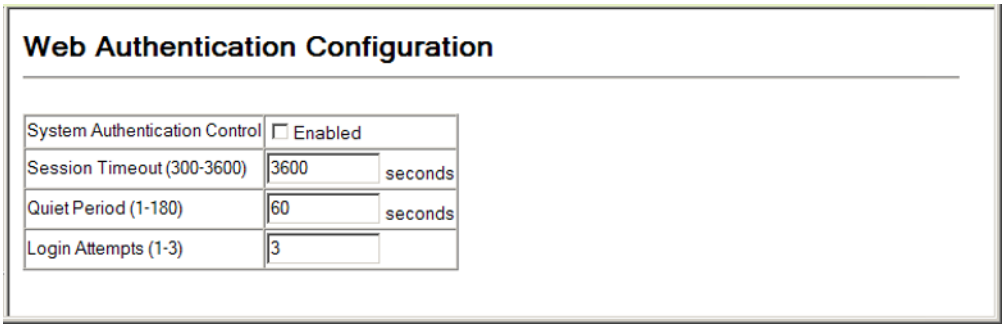
- **Login Attempts** – Configures the amount of times a supplicant may attempt and fail authentication before it must wait the configured quiet period. (Range: 1-3 attempts; Default: 3 attempts)

WEB INTERFACE

To configure global parameters for web authentication:

1. Click Security, Web Authentication, Configuration.
2. Enable web authentication globally on the switch, and adjust any of the protocol parameters as required.
3. Click Apply.

Figure 77: Configuring Global Settings for Web Authentication



CONFIGURING INTERFACE SETTINGS FOR WEB AUTHENTICATION

Use the Security > Web Authentication > Port Configuration page to enable web authentication on a port.

CLI REFERENCES

- "Web Authentication" on page 629

PARAMETERS

These parameters are displayed:

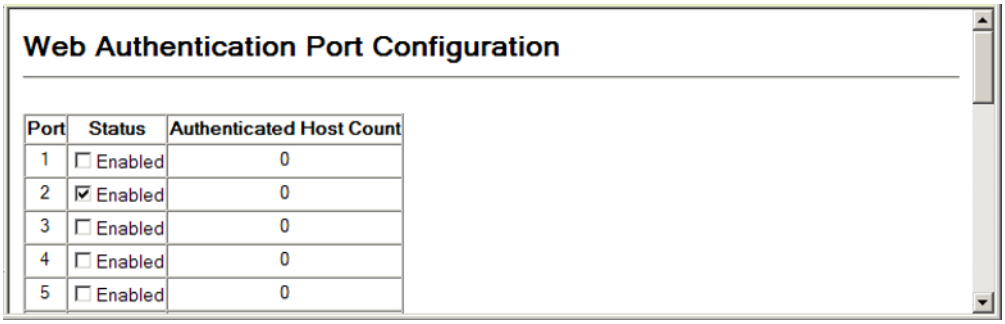
- **Port** – Indicates the port being configured.
- **Status** – Configures the web authentication status for the port.
- **Authenticated Host Counts** – Indicates how many authenticated hosts are connected to the port.

WEB INTERFACE

To enable web authentication for a port:

1. Click Security, Web Authentication, Port Configuration.
2. Set the status box to enabled for any port that requires web authentication, and click Apply

Figure 78: Configuring Interface Settings for Web Authentication



DISPLAYING WEB AUTHENTICATION PORT INFORMATION

Use the Security > Web Authentication > Port Information page to display web authentication information for all ports and connected hosts.

CLI REFERENCES

- "Web Authentication" on page 629

PARAMETERS

These parameters are displayed:

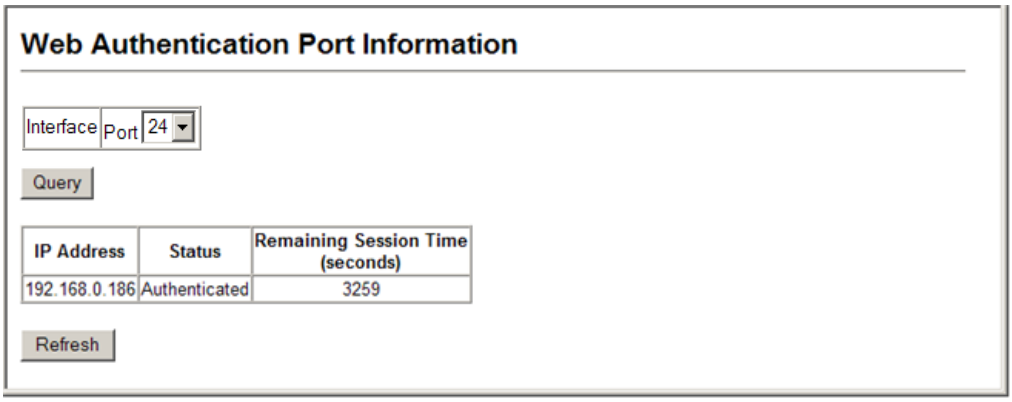
- **Interface** – Indicates the Ethernet port to query.
- **IP Address** – Indicates the IP address of each connected host.
- **Status** – Indicates the authorization status of each connected host.
- **Remaining Session Time** (seconds) – Indicates the remaining time until the current authorization session for the host expires.

WEB INTERFACE

To display web authentication information for a port:

1. Click Security, Web Authentication, Port Information.
2. Select a port from the scroll-down list.
3. Click Query.

Figure 79: Displaying Web Authentication Information for a Port



RE-AUTHENTICATING WEB AUTHENTICATED PORTS

Use the Security > Web Authentication > Re-authentication page to manually force re-authentication of any web-authenticated host connected to any port.

CLI REFERENCES

- "Web Authentication" on page 629

PARAMETERS

These parameters are displayed:

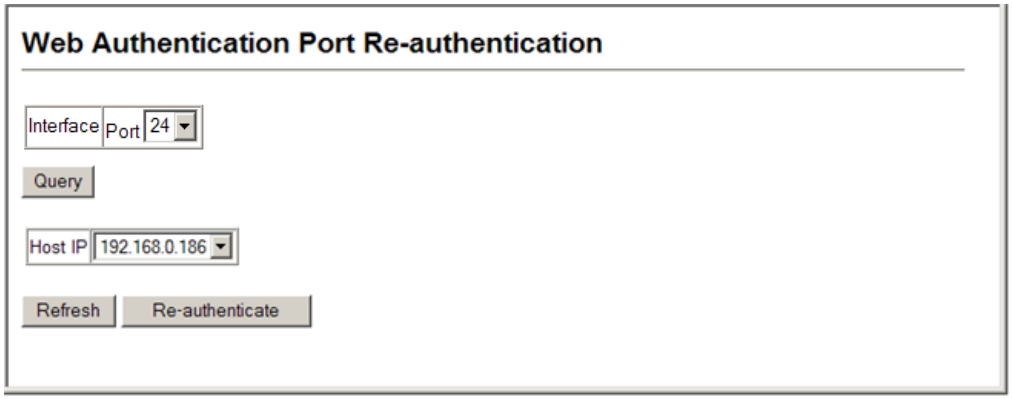
- **Interface** – Indicates the Ethernet port to query.
- **Host IP** – Indicates the IP address of the host selected for re-authentication.
- **Refresh** – Refreshes the list of hosts authenticated on this port.
- **Re-authenticate** – Ends all authenticated web sessions on the selected port, and forces the users to re-authenticate.

WEB INTERFACE

To re-authenticate a host:

1. Click Security, Web Authentication, Re-authentication.
2. Select a port from the Port scroll-down list, and click Query.
3. Select the IP address for a host from the Host IP scroll-down list.
4. Click Re-authenticate.

Figure 80: Re-authenticating a Web-Authenticated Host



NETWORK ACCESS (MAC ADDRESS AUTHENTICATION)

Some devices connected to switch ports may not be able to support 802.1X authentication due to hardware or software limitations. This is often true for devices such as network printers, IP phones, and some wireless access points. The switch enables network access from these devices to be controlled by authenticating device MAC addresses with a central RADIUS server.

NOTE: RADIUS authentication must be activated and configured properly for the MAC Address authentication feature to work properly. (See "Configuring Local/Remote Logon Authentication.")

NOTE: MAC authentication cannot be configured on trunk ports.

CLI REFERENCES

- "Network Access (MAC Address Authentication)" on page 616

COMMAND USAGE

- MAC address authentication controls access to the network by authenticating the MAC address of each host that attempts to connect to a switch port. Traffic received from a specific MAC address is forwarded by the switch only if the source MAC address is successfully authenticated by a central RADIUS server. While authentication for a MAC address is in progress, all traffic is blocked until authentication is completed. On successful authentication, the RADIUS server may optionally assign VLAN and quality of service settings for the switch port.

- When enabled on a port, the authentication process sends a Password Authentication Protocol (PAP) request to a configured RADIUS server. The user name and password are both equal to the MAC address being authenticated. On the RADIUS server, PAP user name and passwords must be configured in the MAC address format XX-XX-XX-XX-XX-XX (all in upper case).

- Authenticated MAC addresses are stored as dynamic entries in the switch secure MAC address table and are removed when the aging time expires. The maximum number of secure MAC addresses supported for the switch system is 1024.

- Configured static MAC addresses are added to the secure address table when seen on a switch port. Static addresses are treated as authenticated without sending a request to a RADIUS server.

- When port status changes to down, all MAC addresses mapped to that port are cleared from the secure MAC address table. Static VLAN assignments are not restored.

- The RADIUS server may optionally return a VLAN identifier list to be applied to the switch port. The following attributes need to be configured on the RADIUS server.
  - **Tunnel-Type** = VLAN
  - **Tunnel-Medium-Type** = 802
  - **Tunnel-Private-Group-ID** = 1u,2t [*VLAN ID list*]

  The VLAN identifier list is carried in the RADIUS "Tunnel-Private-Group-ID" attribute. The VLAN list can contain multiple VLAN identifiers in the format "1u,2t,3u" where "u" indicates an untagged VLAN and "t" a tagged VLAN.

- The RADIUS server may optionally return dynamic QoS assignments to be applied to a switch port for an authenticated user. The "Filter-ID" attribute (attribute 11) can be configured on the RADIUS server to pass the following QoS information:

Table 15: Dynamic QoS Profiles

Profile	Attribute Syntax	Example
DiffServ	**service-policy-in**=*policy-map-name*	service-policy-in=p1
Rate Limit	**rate-limit-input**=*rate*	rate-limit-input=100 (in units of Kbps)
802.1p	**switchport-priority-default**=*value*	switchport-priority-default=2

- Multiple profiles can be specified in the Filter-ID attribute by using a semicolon to separate each profile.

  For example, the attribute "service-policy-in=pp1;rate-limit-input=100" specifies that the diffserv profile name is "pp1," and the ingress rate limit profile value is 100 kbps.

- If duplicate profiles are passed in the Filter-ID attribute, then only the first profile is used.

  For example, if the attribute is "service-policy-in=p1;service-policy-in=p2", then the switch applies only the DiffServ profile "p1."

- Any unsupported profiles in the Filter-ID attribute are ignored.

  For example, if the attribute is "map-ip-dscp=2:3;service-policy-in=p1," then the switch ignores the "map-ip-dscp" profile.

- When authentication is successful, the dynamic QoS information may not be passed from the RADIUS server due to one of the following conditions (authentication result remains unchanged):
  - The Filter-ID attribute cannot be found to carry the user profile.
  - The Filter-ID attribute is empty.
  - The Filter-ID attribute format for dynamic QoS assignment is unrecognizable (can not recognize the whole Filter-ID attribute).

- Dynamic QoS assignment fails and the authentication result changes from success to failure when the following conditions occur:
  - Illegal characters found in a profile value (for example, a non-digital character in an 802.1p profile value).
  - Failure to configure the received profiles on the authenticated port.
- When the last user logs off on a port with a dynamic QoS assignment, the switch restores the original QoS configuration for the port.
- When a user attempts to log into the network with a returned dynamic QoS profile that is different from users already logged on to the same port, the user is denied access.
- While a port has an assigned dynamic QoS profile, any manual QoS configuration changes only take effect after all users have logged off the port.

NOTE: Any configuration changes for dynamic QoS are not saved to the switch configuration file.

CONFIGURING GLOBAL SETTINGS FOR NETWORK ACCESS

MAC address authentication is configured on a per-port basis, however there are two configurable parameters that apply globally to all ports on the switch. Use the Security > Network Access (Configure Global) page to configure MAC address authentication aging and reauthentication time.

CLI REFERENCES

- "Network Access (MAC Address Authentication)" on page 616

PARAMETERS

These parameters are displayed:

- **Authenticated Age** – The secure MAC address table aging time. This parameter setting is the same as switch MAC address table aging time and is only configurable from the Address Table > Aging Time page (see page 296). (Default: 300 seconds)
- **MAC Address Reauthentication Time** – Sets the time period after which a connected host must be reauthenticated. When the reauthentication time expires for a secure MAC address, it is reauthenticated with the RADIUS server. During the reauthentication process traffic through the port remains unaffected. (Range: 120-1000000 seconds; Default: 1800 seconds)
- **MAC Address Aging** – Enables aging for authenticated MAC addresses stored in the secure MAC address table. (Default: Disabled)

  This parameter applies to authenticated MAC addresses configured by the MAC Address Authentication process described in this section, as well as to any secure MAC addresses authenticated by 802.1X,

regardless of the 802.1X Operation Mode (Single-Host, Multi-Host, or MAC-Based authentication as described on page 203).

Authenticated MAC addresses are stored as dynamic entries in the switch's secure MAC address table and are removed when the aging time expires.

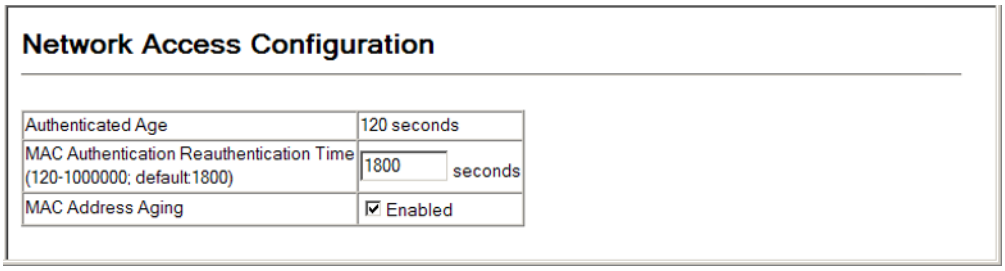
The maximum number of secure MAC addresses supported for the switch system is 1024.

WEB INTERFACE

To configure aging status and reauthentication time for MAC address authentication:

1. Click Security, Network Access, Configuration.
2. Enable or disable aging for secure addresses, and modify the reauthentication time as required.
3. Click Apply.

Figure 81: Configuring Global Settings for Network Access



CONFIGURING NETWORK ACCESS FOR PORTS

Use the Security > Network Access > Port Configuration page to configure MAC authentication on switch ports, including enabling address authentication, setting the maximum MAC count, and enabling dynamic VLAN or dynamic QoS assignments.

CLI REFERENCES

- "Network Access (MAC Address Authentication)" on page 616

PARAMETERS

These parameters are displayed:

- **Mode** – Enables MAC authentication on a port. (Default: disabled)
- **Max MAC Count** – Sets the maximum number of MAC addresses that can be authenticated on a port via MAC authentication; that is, the Network Access process described in this section. (Range: 1-2048; Default: 2048)

  The maximum number of MAC addresses per port is 2048, and the maximum number of secure MAC addresses supported for the switch system is 2048. When the limit is reached, all new MAC addresses are treated as authentication failures.

- **Guest VLAN** – Specifies the VLAN to be assigned to the port when 802.1X Authentication fails. (Range: 0-4094, where 0 means disabled; Default: disabled)

  The VLAN must already be created and active (see "Configuring VLAN Groups"). Also, when used with 802.1X authentication, intrusion action must be set for "Guest VLAN" (see "Configuring Authenticator Port Settings for 802.1X").

- **MAC Filter ID** – Allows a MAC Filter to be assigned to the port. MAC addresses or MAC address ranges present in a selected MAC Filter are exempt from authentication on the specified port (as described under "Configuring a MAC Address Filter"). (Range: 1-64; Default: None)

- **Dynamic VLAN** – Enables dynamic VLAN assignment for an authenticated port. When enabled, any VLAN identifiers returned by the RADIUS server are applied to the port, providing the VLANs have already been created on the switch. (GVRP is not used to create the VLANs.) (Default: Enabled)

  The VLAN settings specified by the first authenticated MAC address are implemented for a port. Other authenticated MAC addresses on the port must have the same VLAN configuration, or they are treated as authentication failures.

  If dynamic VLAN assignment is enabled on a port and the RADIUS server returns no VLAN configuration, the authentication is still treated as a success, and the host is assigned to the default untagged VLAN.

  When the dynamic VLAN assignment status is changed on a port, all authenticated addresses are cleared from the secure MAC address table.

- **Dynamic QoS** – Enables dynamic QoS assignment for an authenticated port. (Default: Disabled)

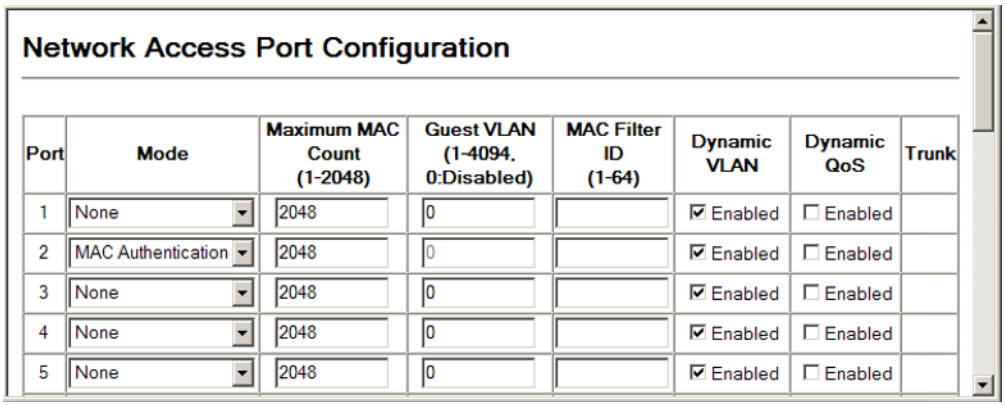
- **Trunk** – Shows if this port is a member of a trunk.

WEB INTERFACE

To configure MAC authentication on switch ports:

1. Click Security, Network Access, Port Configuration.
2. Make any configuration changes required to enable address authentication on a port, set the maximum number of secure addresses supported, the guest VLAN to use when 802.1X Authentication fails, and the dynamic VLAN and QoS assignments.
3. Click Apply.

Figure 82: Configuring Interface Settings for Network Access



CONFIGURING PORT LINK DETECTION

Use the Security > Network Access > Port Link Detection page to send an SNMP trap and/or shut down a port when a link event occurs.

CLI REFERENCES

- "Network Access (MAC Address Authentication)" on page 616

PARAMETERS

These parameters are displayed:

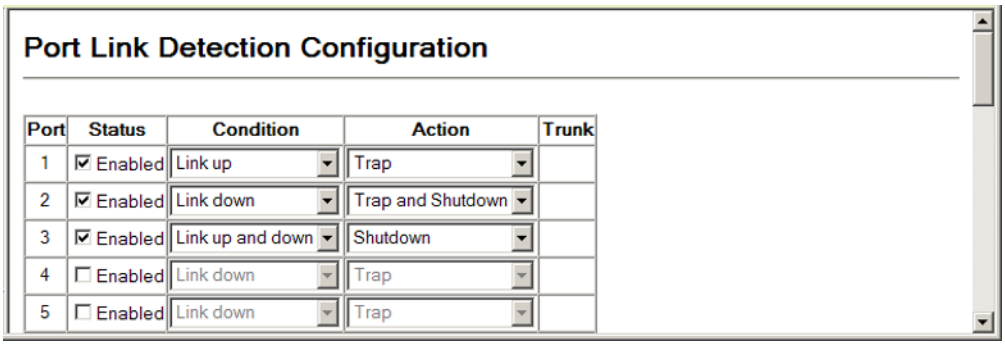
- **Port** – Indicates a port on this switch.
- **Status** – Configures whether Link Detection is enabled or disabled for a port.
- **Condition** – The link event type which will trigger the port action.
  - **Link up** – Only link up events will trigger the port action.
  - **Link down** – Only link down events will trigger the port action.
  - **Link up and down** – All link up and link down events will trigger the port action.
- **Action** – The switch can respond in three ways to a link up or down trigger event.
  - **Trap** – An SNMP trap is sent.
  - **Trap and shutdown** – An SNMP trap is sent and the port is shut down.
  - **Shutdown** – The port is shut down.
- **Trunk** – Indicates if the port is a trunk member.

WEB INTERFACE

To configure link detection on switch ports:

1. Click Security, Network Access, Port Link Detection.
2. Modify the link detection status, trigger condition, and the response for any port.
3. Click Apply.

Figure 83: Configuring Link Detection for Network Access



DISPLAYING SECURE MAC ADDRESS INFORMATION

Use the Security > Network Access > MAC Address Information page to display the authenticated MAC addresses stored in the secure MAC address table. Information on the secure MAC entries can be displayed and selected entries can be removed from the table.

CLI REFERENCES

- "Network Access (MAC Address Authentication)" on page 616

PARAMETERS

These parameters are displayed:

- **Network Access MAC Address Count** – The number of MAC addresses currently in the secure MAC address table.
- **Query By** – Specifies parameters to use in the MAC address query.
  - **Port** – Specifies a port interface.
  - **MAC Address** – Specifies a specific MAC address.
  - **Attribute** – Displays static or dynamic addresses.
  - **Address Table Sort Key** – Sorts the information displayed based on MAC address or port interface.

Authenticated MAC Address List

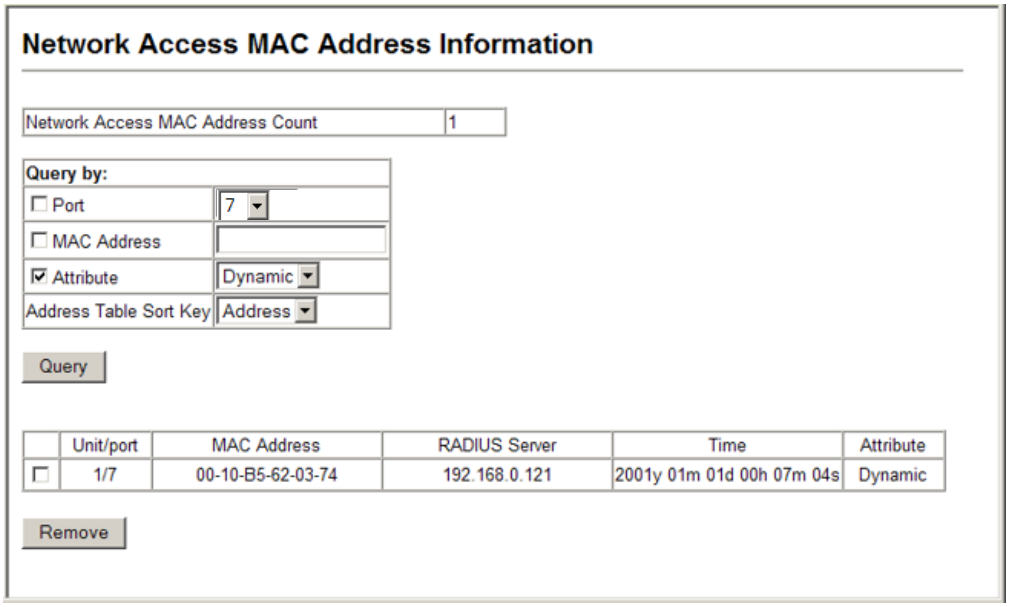
- **Unit/Port** – The port associated with a secure MAC address.
- **MAC Address** – The authenticated MAC address.
- **RADIUS Server** – The IP address of the RADIUS server that authenticated the MAC address.
- **Time** – The time when the MAC address was last authenticated.
- **Attribute** – Indicates a static or dynamic address.

WEB INTERFACE

To display the authenticated MAC addresses stored in the secure MAC address table:

1. Click Security, Network Access, MAC Address Information.
2. Use the sort key to display addresses based MAC address or interface.
3. Restrict the displayed addresses by entering a specific address in the MAC Address field, specifying a port in the Interface field, or setting the address type to static or dynamic in the Attribute field.
4. Click Query.

Figure 84: Showing Addresses Authenticated for Network Access



CONFIGURING A MAC ADDRESS FILTER

Use the Security > Network Access > MAC Filter Configuration page to designate specific MAC addresses or MAC address ranges as exempt from authentication. MAC addresses present in MAC Filter tables activated on a port are treated as pre-authenticated on that port.

CLI REFERENCES

- "Network Access (MAC Address Authentication)" on page 616

COMMAND USAGE

- Specified MAC addresses are exempt from authentication.
- Up to 64 filter tables can be defined.
- There is no limitation on the number of entries used in a filter table.

PARAMETERS

These parameters are displayed:

- **Filter ID** (1-64) - *top*
  - **ALL** – Selects all configured MAC filter tables.
  - **Filter ID** – Selects all entries associated with a MAC Filter ID.
- **Query** – Displays all entries in the specified table(s).

Rule Configuration

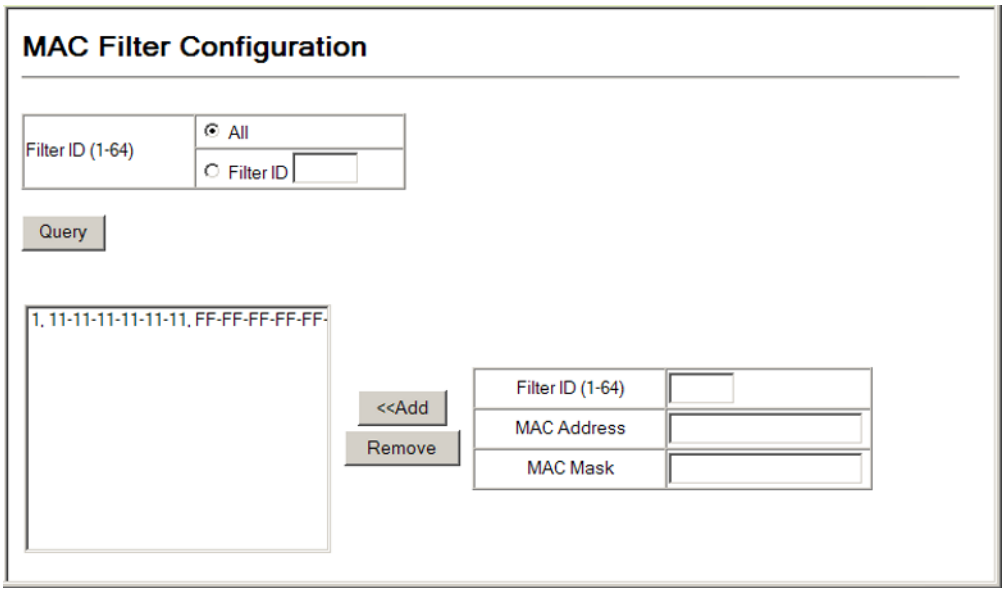
- **Filter ID** (1-64) – Adds or removes a rule for the specified filter.
- **MAC Address** – The filter rule will check ingress packets against the entered MAC address or range of MAC addresses (as defined by the MAC Address Mask).
- **MAC Address Mask** – The filter rule will check for the range of MAC addresses defined by the MAC address bit mask. If you omit the mask, the system will assign the default mask of an exact match. (Range: 000000000000 - FFFFFFFFFFFF; Default: FFFFFFFFFFFF)

WEB INTERFACE

To add a MAC address filter for MAC authentication:

1. Click Security, Network Access, MAC Filter Configuration.
2. Enter a filter ID, MAC address, and optional mask.
3. Click Add.

Figure 85: Configuring a MAC Address Filter for Network Access



ACCESS CONTROL LISTS

Access Control Lists (ACL) provide packet filtering for IPv4 frames (based on address, protocol, Layer 4 protocol port number or TCP control code), IPv6 frames (based on address or DSCP traffic class), or any frames (based on MAC address or Ethernet type). To filter incoming packets, first create an access list, add the required rules, and then bind the list to a specific port.

Configuring Access Control Lists –

An ACL is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the packet is accepted.

COMMAND USAGE

The following restrictions apply to ACLs:

- The maximum number of ACLs is 64.
- The maximum number of rules per system is 512 rules.
- An ACL can have up to 64 rules. However, due to resource restrictions, the average number of rules bound to the ports should not exceed 20.

NOTE: The CLI includes a control function which restricts access lists to only extended rules, or permits both standard and extended rules. For a detailed description of this feature, refer to the access-list rule-mode command.

The default setting only permits extended rules, storing any standard rules entered through the web or command line interface in extended rule format.

SETTING THE ACL NAME AND TYPE

Use the Security > ACL > Configuration page to designate the name and type of an ACL.

CLI REFERENCES

- "access-list ip" on page 660
- "access-list ipv6" on page 667
- "access-list mac" on page 672
- "access-list arp" on page 677

PARAMETERS

These parameters are displayed:

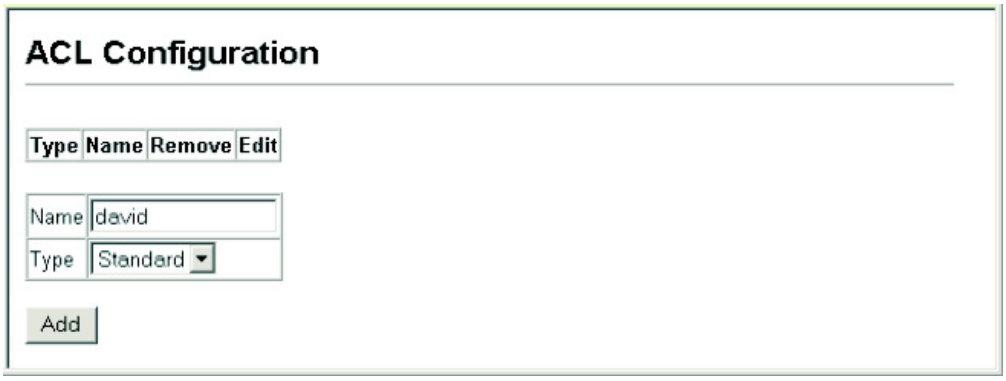
- **ACL Name** – Name of the ACL. (Maximum length: 15 characters)
- **Type** – The following filter modes are supported:
  - **IP Standard**: IPv4 ACL mode filters packets based on the source IPv4 address.
  - **IP Extended**: IPv4 ACL mode filters packets based on the source or destination IPv4 address, as well as the protocol type and protocol port number. If the "TCP" protocol is specified, then you can also filter packets based on the TCP control code.
  - **IPv6 Standard**: IPv6 ACL mode filters packets based on the source IPv6 address.
  - **IPv6 Extended**: IPv6 ACL mode filters packets based on the source or destination IP address, as well as the DSCP traffic class.
  - **MAC** – MAC ACL mode filters packets based on the source or destination MAC address and the Ethernet frame type (RFC 1060).
  - **ARP** – ARP ACL specifies static IP-to-MAC address bindings used for ARP inspection (see "ARP Inspection").

WEB INTERFACE

To configure the name and type of an ACL:

1. Click Security, ACL, Configuration.
2. Fill in the ACL Name field, and select the ACL type.
3. Click Apply.

Figure 86: Creating an ACL



CONFIGURING A STANDARD IPV4 ACL

Use the Security > ACL > Configure (Standard ACL) page to configure a Standard IPv4 ACL.

CLI REFERENCES

- "permit, deny (Standard IP ACL)" on page 662
- "show ip access-list" on page 666

PARAMETERS

These parameters are displayed:

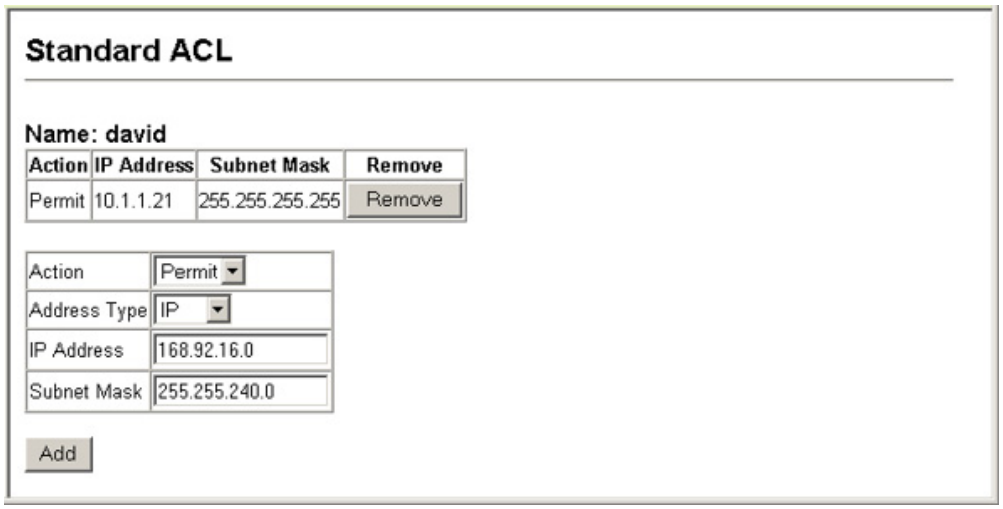
- **Name** – Shows the name of the selected ACL.
- **Action** – An ACL can contain any combination of permit or deny rules.
- **Address Type** – Specifies the source IP address. Use "Any" to include all possible addresses, "Host" to specify a specific host address in the Address field, or "IP" to specify a range of addresses with the IP Address and Subnet Mask fields. (Options: Any, Host, IP; Default: Any)
- **IP Address** – Source IP address.
- **Subnet Mask** – A subnet mask containing four integers from 0 to 255, each separated by a period. The mask uses 1 bits to indicate "match" and 0 bits to indicate "ignore." The mask is bitwise ANDed with the specified source IP address, and compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

WEB INTERFACE

To add rules to a Standard IP ACL:

1. Click Security, ACL, Configuration.
2. Click Edit to open the configuration page for the required entry.
3. Specify the action (i.e., Permit or Deny).
4. Select the address type (Any, Host, or IP).
5. If you select "Host," enter a specific address. If you select "IP," enter a subnet address and the mask for an address range.
6. Click Add.

Figure 87: Configuring a Standard IPv4 ACL



CONFIGURING AN EXTENDED IPV4 ACL

Use the Security > ACL > Configure (Extended ACL) page to configure an Extended IPv4 ACL.

CLI REFERENCES

- "permit, deny (Extended IPv4 ACL)" on page 663
- "show ip access-list" on page 666

PARAMETERS

These parameters are displayed:

- **Name** – Shows the name of the selected ACL.
- **Action** – An ACL can contain any combination of permit or deny rules.
- **Source/Destination Address Type** – Specifies the source or destination IP address. Use "Any" to include all possible addresses, "Host" to specify a specific host address in the Address field, or "IP" to

specify a range of addresses with the Address and Subnet Mask fields. (Options: Any, Host, IP; Default: Any)

- **Source/Destination IP Address** – Source or destination IP address.
- **Source/Destination Subnet Mask** – Subnet mask for source or destination address. (See the description for Subnet Mask on page 226.)
- **Service Type** – Packet priority settings based on the following criteria:
  - **ToS** – Type of Service level. (Range: 0-15)
  - **Precedence** – IP precedence level. (Range: 0-7)
  - **DSCP** – DSCP priority level. (Range: 0-63)
- **Protocol** – Specifies the protocol type to match as TCP, UDP or Others, where others indicates a specific protocol number (0-255). (Options: TCP, UDP, Others; Default: TCP)
- **Source/Destination Port** – Source/destination port number for the specified protocol type. (Range: 0-65535)
- **Source/Destination Port Bit Mask** – Decimal number representing the port bits to match. (Range: 0-65535)
- **Control Code** – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)
- **Control Code Bit Mask** – Decimal number representing the code bits to match. (Range: 0-63)

  The control bit mask is a decimal number (for an equivalent binary bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit "1" means to match a bit and "0" means to ignore a bit. The following bits may be specified:

  - 1 (fin) – Finish
  - 2 (syn) – Synchronize
  - 4 (rst) – Reset
  - 8 (psh) – Push
  - 16 (ack) – Acknowledgement
  - 32 (urg) – Urgent pointer

  For example, use the code value and mask below to catch packets with the following flags set:

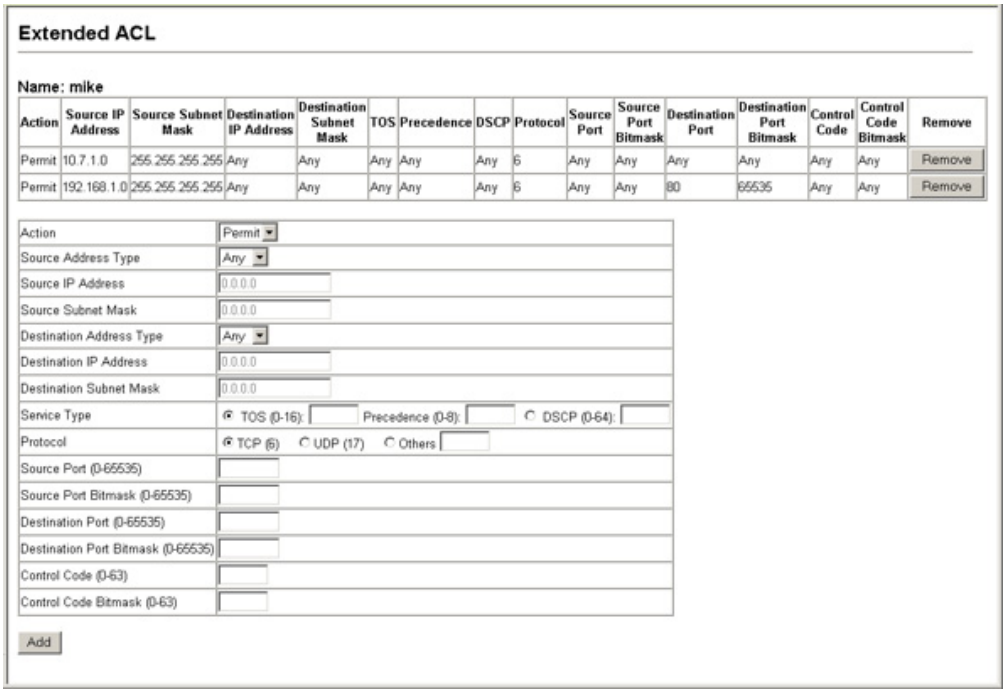
  - SYN flag valid, use control-code 2, control bit mask 2
  - Both SYN and ACK valid, use control-code 18, control bit mask 18
  - SYN valid and ACK invalid, use control-code 2, control bit mask 18

WEB INTERFACE

To add rules to an Extended IP ACL:

1. Click Security, ACL, Configuration.
2. Click Edit to open the configuration page for the required entry.
3. Specify the action (i.e., Permit or Deny).
4. Select the address type (Any, Host, or IP).
5. If you select "Host," enter a specific address. If you select "IP," enter a subnet address and the mask for an address range.
6. Set any other required criteria, such as service type, protocol type, or control code.
7. Click Add.

Figure 88: Configuring an Extended IPv4 ACL



CONFIGURING A STANDARD IPV6 ACL

Use the Security > ACL > Configure (IPv6 Standard ACL) page to configure a Standard IPv6 ACL.

CLI REFERENCES

- "permit, deny (Standard IPv6 ACL)" on page 668
- "show ipv6 access-list" on page 670

PARAMETERS

These parameters are displayed in the web interface:

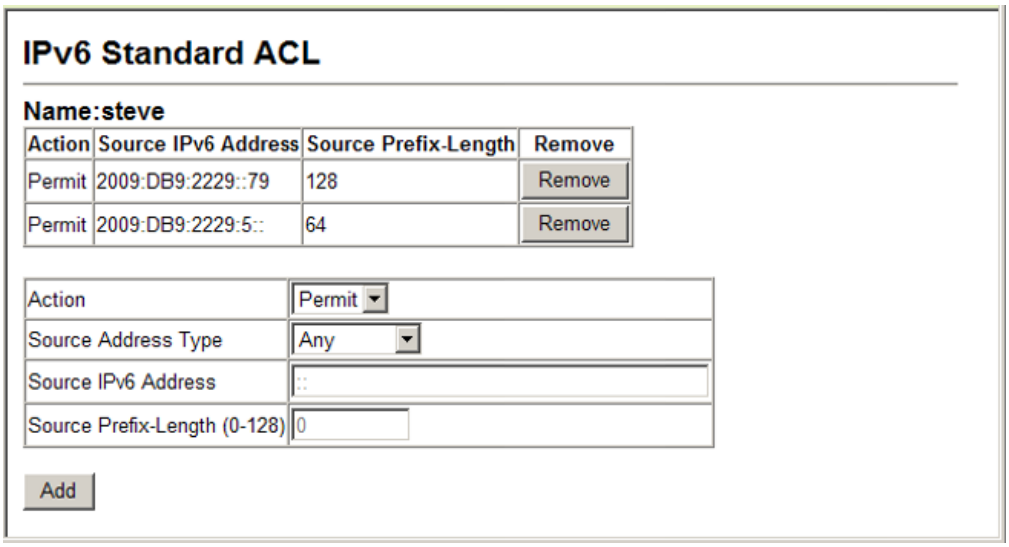
- **Name** – Shows the name of the selected ACL.
- **Action** – An ACL can contain any combination of permit or deny rules.
- **Source Address Type** – Specifies the source IP address. Use "Any" to include all possible addresses, "Host" to specify a specific host address in the Address field, or "IPv6-prefix" to specify a range of addresses. (Options: Any, Host, IPv6-prefix; Default: Any)
- **Source IPv6 Address** – An IPv6 source address or network class. The address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- **Source Prefix-Length** – A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

WEB INTERFACE

To add rules to a Standard IPv6 ACL:

1. Click Security, ACL.
2. Click Edit to open the configuration page for the required entry.
3. Specify the action (i.e., Permit or Deny).
4. Select the source address type (Any, Host, or IPv6-prefix).
5. If you select "Host," enter a specific address. If you select "IPv6-prefix," enter a subnet address and the prefix length.
6. Click Add.

Figure 89: Configuring a Standard IPv6 ACL



CONFIGURING AN EXTENDED IPV6 ACL

Use the Security > ACL > Configure (IPv6 Extended ACL) page to configure an Extended IPv6 ACL.

CLI REFERENCES

- "permit, deny (Extended IPv6 ACL)" on page 669
- "show ipv6 access-list" on page 670

PARAMETERS

These parameters are displayed in the web interface:

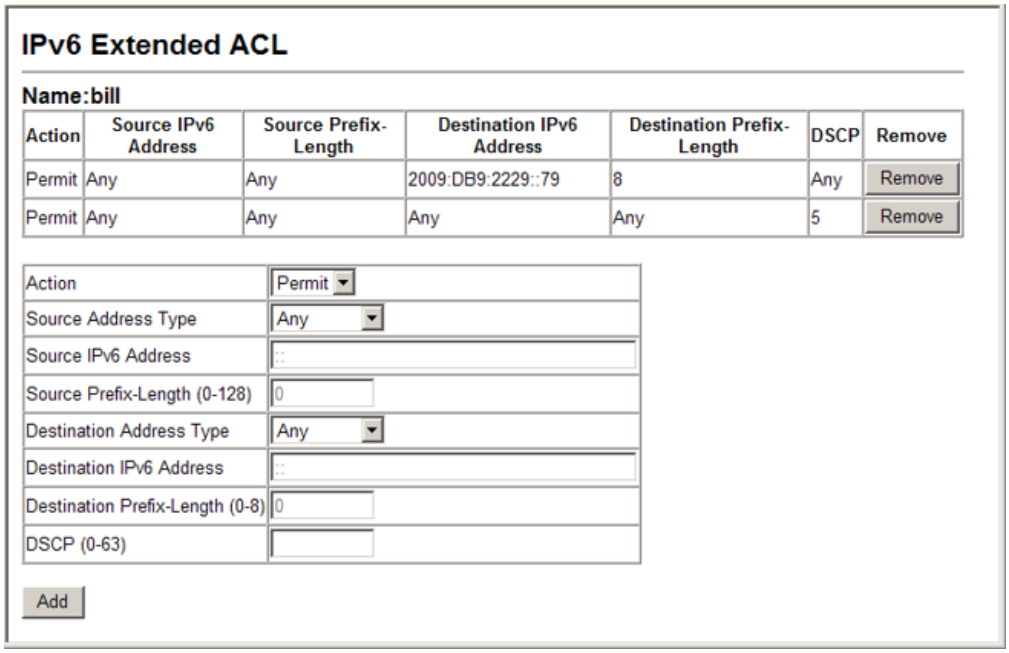
- **Name** – Shows the name of the selected ACL.
- **Action** – An ACL can contain any combination of permit or deny rules.
- **Source/Destination Address Type** – Specifies the source or destination IP address. Use "Any" to include all possible addresses, "Host" to specify a specific host address in the Source IPv6 Address field, or "IPv6-prefix" to specify a range of addresses. (Options: Any, Host, IPv6-prefix; Default: Any)
- **Source/Destination IP Address** – An IPv6 address or network class. The address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (The switch only checks the first 64 bits of the destination address.)
- **Source/Destination Prefix-Length** – A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix; i.e., the network portion of the address. (Range: 0-8)
- **DSCP** – DSCP traffic class. (Range: 0-63)

WEB INTERFACE

To add rules to an Extended IPv6 ACL:

1. Click Security, ACL.
2. Click Edit to open the configuration page for the required entry.
3. Specify the action (i.e., Permit or Deny).
4. Select the address type (Any, Host, or IPv6-prefix).
5. If you select "Host," enter a specific address. If you select "IPv6-prefix," enter a subnet address and prefix length.
6. Set the DSCP traffic class if required.
7. Click Add.

Figure 90: Configuring an Extended IPv6 ACL



CONFIGURING A MAC ACL

Use the Security > ACL > Configure (MAC ACL) page to configure a MAC ACL based on hardware addresses, packet format, and Ethernet type.

CLI REFERENCES

- "permit, deny (MAC ACL)" on page 673
- "show ip access-list" on page 666

PARAMETERS

These parameters are displayed:

- **Name** – Shows the name of the selected ACL.

- **Action** – An ACL can contain any combination of permit or deny rules.
- **Source/Destination Address Type** – Use "Any" to include all possible addresses, "Host" to indicate a specific MAC address, or "MAC" to specify an address range with the Address and Bit Mask fields. (Options: Any, Host, MAC; Default: Any)
- **Source/Destination MAC Address** – Source or destination MAC address.
- **Source/Destination Bit Mask** – Hexadecimal mask for source or destination MAC address.
- **CoS** – CoS value. (Range: 0-7, where 7 is the highest priority)
- **CoS Bit Mask** – CoS bitmask. (Range: 0-7)
- **VID** – VLAN ID. (Range: 1-4094)
- **VID Bit Mask** – VLAN bit mask. (Range: 0-4094)
- **Ethernet Type** – This option can only be used to filter Ethernet II formatted packets. (Range: 600-ffff hex.)

  A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX).
- **Ethernet Type Bit Mask** – Protocol bit mask. (Range: 600-ffff hex.)
- **Packet Format** – This attribute includes the following packet types:
  - **Any** – Any Ethernet packet type.
  - **Untagged-eth2** – Untagged Ethernet II packets.
  - **Untagged-802.3** – Untagged Ethernet 802.3 packets.
  - **tagged-eth2** – Tagged Ethernet II packets.
  - **Tagged-802.3** – Tagged Ethernet 802.3 packets.

WEB INTERFACE

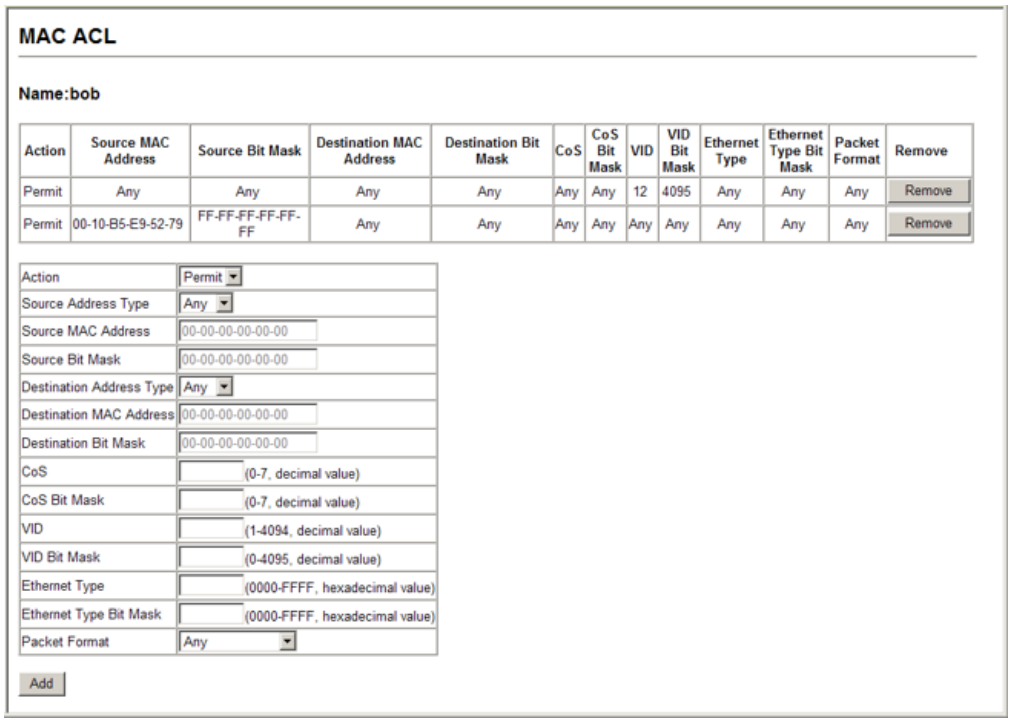
To add rules to a MAC ACL:

1. Click Security, ACL.
2. Click Edit to open the configuration page for the required entry.
3. Specify the action (i.e., Permit or Deny).
4. Select the address type (Any, Host, or MAC).
5. If you select "Host," enter a specific address (e.g., 11-22-33-44-55-66). If you select "MAC," enter a base address and a hexadecimal bit mask for an address range.

6. Set any other required criteria, such as VID, Ethernet type, or packet format.

7. Click Add.

Figure 91: Configuring a MAC ACL



CONFIGURING AN ARP ACL

Use the Security > ACL > Configure (ARP ACL) page to configure ACLs based on ARP message addresses. ARP Inspection can then use these ACLs to filter suspicious traffic (see "Configuring Global Settings for ARP Inspection").

CLI REFERENCES

- "permit, deny (ARP ACL)" on page 678
- "show ip access-list" on page 666

PARAMETERS

These parameters are displayed:

- **Name** – Shows the name of the selected ACL.
- **Action** – An ACL can contain any combination of permit or deny rules.
- **Packet Type** – Indicates an ARP request, ARP response, or either type. (Range: Request, Response, All; Default: Request)
- **Sender/Target IP Address Type** – Specifies the source or destination IPv4 address. Use "Any" to include all possible addresses, "Host" to specify a specific host address in the Address field, or "IP" to

specify a range of addresses with the Address and Mask fields. (Options: Any, Host, IP; Default: Any)

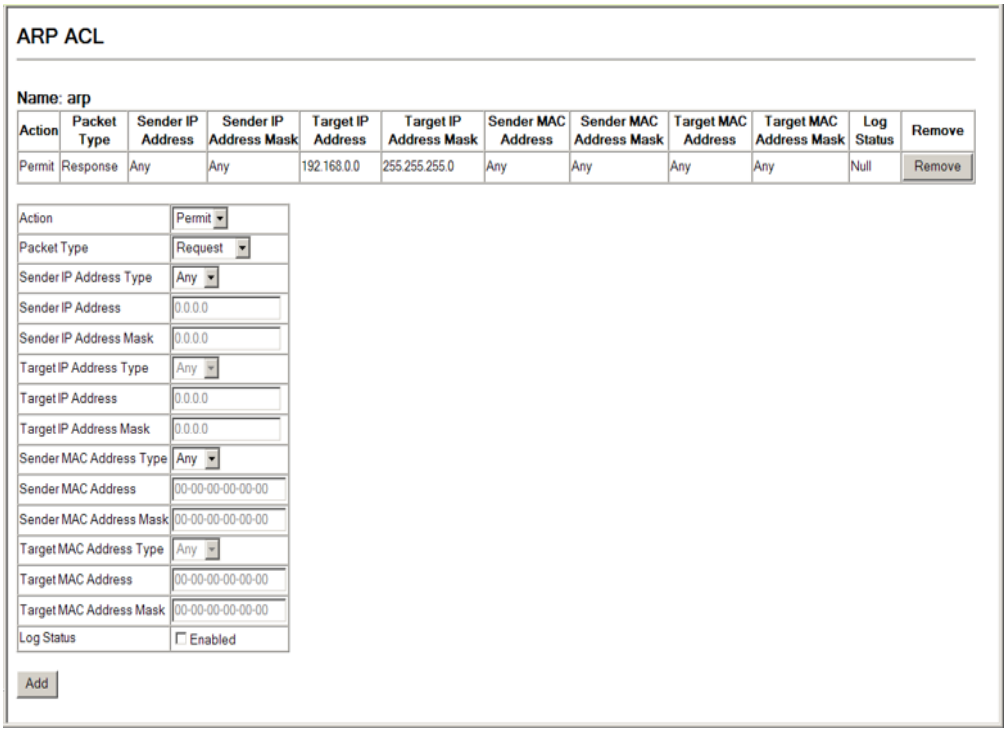
- **Sender/Target IP Address** – Source or destination IP address.
- **Sender/Target IP Address Mask** – Subnet mask for source or destination address. (See the description for Subnet Mask on page 226.)
- **Sender/Target MAC Address Type** – Use "Any" to include all possible addresses, "Host" to indicate a specific MAC address, or "MAC" to specify an address range with the Address and Mask fields. (Options: Any, Host, MAC; Default: Any)
- **Sender/Target MAC Address** – Source or destination MAC address.
- **Sender/Target MAC Address Mask** – Hexadecimal mask for source or destination MAC address.
- **Log Status** – Logs a packet when it matches the access control entry.

WEB INTERFACE

To add rules to an ARP ACL:

1. Click Security, ACL.
2. Click Edit to open the configuration page for the required entry.
3. Specify the action (i.e., Permit or Deny).
4. Select the packet type (Request, Response, All).
5. Select the address type (Any, Host, or IP).
6. If you select "Host," enter a specific address (e.g., 11-22-33-44-55-66). If you select "IP," enter a base address and a hexadecimal bit mask for an address range.
7. Enable logging if required.
8. Click Add.

Figure 92: Configuring a ARP ACL



BINDING A PORT TO AN ACCESS CONTROL LIST

After configuring ACLs, use the Security > ACL > Port Binding page to bind the ports that need to filter traffic to the appropriate ACLs. You can assign one IP access list and one MAC access list to any port.

CLI REFERENCES

- "ip access-group" on page 665
- "ipv6 access-group" on page 671
- "mac access-group" on page 675

COMMAND USAGE

- This switch supports ACLs for ingress filtering only.
- You only bind one ACL to any port for ingress filtering.

PARAMETERS

These parameters are displayed:

- **Port** – Fixed port or SFP module. (Range: 1-28/52)
- **IP** – Specifies the IP ACL to bind to a port.
- **MAC** – Specifies the MAC ACL to bind to a port.
- **IPv6** – Specifies the IPv6 ACL to bind to a port.
- **IN** – ACL for ingress packets.

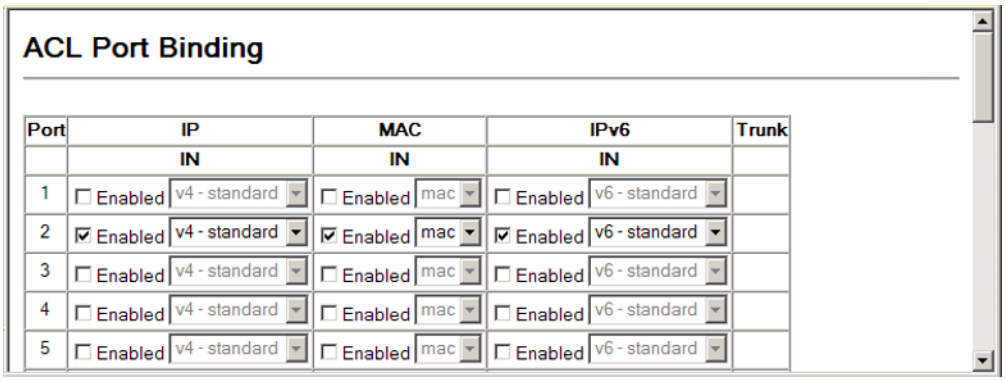
- Trunk – Indicates if a port is a member of a trunk. To create trunks and select port members, see "Trunk Configuration."

WEB INTERFACE

To bind an ACL to a port:

1. Click Security, ACL, Port Binding.
2. Mark the Enabled check box for the port you want to bind to an ACL for ingress traffic, and select the required ACL from the drop-down list.
3. Click Apply.

Figure 93: Binding a Port to an ACL



SHOWING TCAM UTILIZATION

Use the Security > ACL > TCAM Utilization page to show utilization parameters for TCAM (Ternary Content Addressable Memory), including the number policy control entries in use, the number of free entries, and the overall percentage of TCAM in use.

CLI REFERENCES

- "show access-list tcam-utilization" on page 464

COMMAND USAGE

Policy control entries (PCEs) are used by various system functions which rely on rule-based searches, including Access Control Lists (ACLs), IP Source Guard filter rules, Quality of Service (QoS) processes, or traps.

For example, when binding an ACL to a port, each rule in an ACL will use two PCEs; and when setting an IP Source Guard filter rule for a port, the system will also use two PCEs.

PARAMETERS

These parameters are displayed:

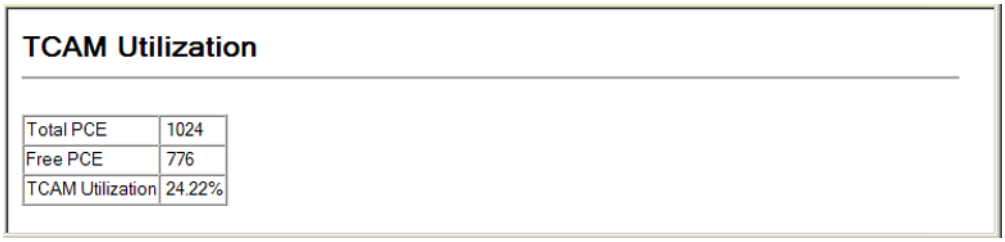
- **Total PCE** – The number policy control entries in use.
- **Free PCE** – The number of policy control entries available for use.
- **TCAM Utilization** – The overall percentage of TCAM in use.

WEB INTERFACE

To show information on TCAM utilization:

1. Click Security, ACL, TCAM Utilization.

Figure 94: Showing TCAM Utilization



ARP INSPECTION

ARP Inspection is a security feature that validates the MAC Address bindings for Address Resolution Protocol packets. It provides protection against ARP traffic with invalid MAC-to-IP address bindings, which forms the basis for certain "man-in-the-middle" attacks. This is accomplished by intercepting all ARP requests and responses and verifying each of these packets before the local ARP cache is updated or the packet is forwarded to the appropriate destination. Invalid ARP packets are dropped.

ARP Inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database – the DHCP snooping binding database (see "DHCP Snooping"). This database is built by DHCP snooping if it is enabled on globally on the switch and on the required VLANs. ARP Inspection can also validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured addresses (see "Configuring an ARP ACL").

COMMAND USAGE

Enabling & Disabling ARP Inspection

- ARP Inspection is controlled on a global and VLAN basis.
- By default, ARP Inspection is disabled both globally and on all VLANs.
  - If ARP Inspection is globally enabled, then it becomes active only on the VLANs where it has been enabled.
  - When ARP Inspection is enabled globally, all ARP request and reply packets on inspection-enabled VLANs are redirected to the CPU and their switching behavior handled by the ARP Inspection engine.
  - If ARP Inspection is disabled globally, then it becomes inactive for all VLANs, including those where inspection is enabled.

- When ARP Inspection is disabled, all ARP request and reply packets will bypass the ARP Inspection engine and their switching behavior will match that of all other packets.
- Disabling and then re-enabling global ARP Inspection will not affect the ARP Inspection configuration of any VLANs.
- When ARP Inspection is disabled globally, it is still possible to configure ARP Inspection for individual VLANs. These configuration changes will only become active after ARP Inspection is enabled globally again.

- The ARP Inspection engine in the current firmware version does not support ARP Inspection on trunk ports.

CONFIGURING GLOBAL SETTINGS FOR ARP INSPECTION

Use the Security > ARP Inspection > Configuration page to enable ARP inspection globally for the switch, to validate address information in each packet, and configure logging.

CLI REFERENCES

- "ARP Inspection" on page 649

COMMAND USAGE

ARP Inspection Validation

- By default, ARP Inspection Validation is disabled.
- Specifying at least one of the following validations enables ARP Inspection Validation globally. Any combination of the following checks can be active concurrently.
  - Destination MAC – Checks the destination MAC address in the Ethernet header against the target MAC address in the ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.
  - IP – Checks the ARP body for invalid and unexpected IP addresses. These addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, while target IP addresses are checked only in ARP responses.
  - Source MAC – Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

ARP Inspection Logging

- By default, logging is active for ARP Inspection, and cannot be disabled.
- The administrator can configure the log facility rate.
- When the switch drops a packet, it places an entry in the log buffer, then generates a system message on a rate-controlled basis. After the system message is generated, the entry is cleared from the log buffer.
- Each log entry contains flow information, such as the receiving VLAN, the port number, the source and destination IP addresses, and the source and destination MAC addresses.
- If multiple, identical invalid ARP packets are received consecutively on the same VLAN, then the logging facility will only generate one entry in the log buffer and one corresponding system message.
- If the log buffer is full, the oldest entry will be replaced with the newest entry.

PARAMETERS

These parameters are displayed:

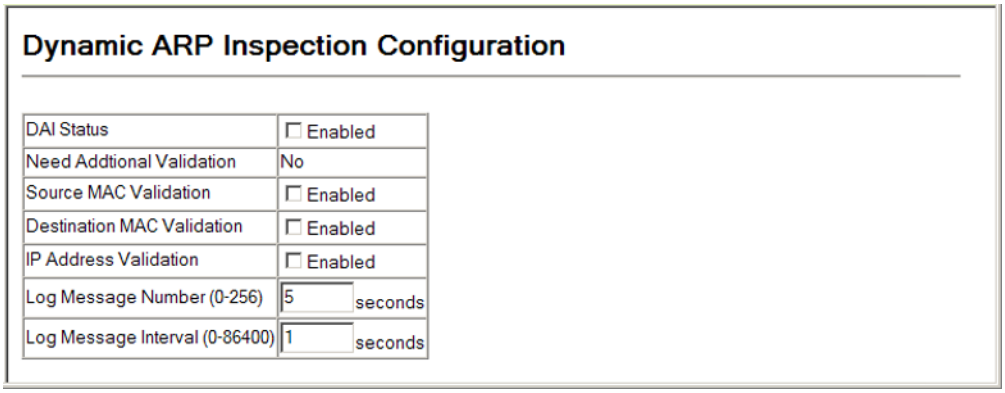
- **DAI Status** – Enables Dynamic ARP Inspection globally. (Default: Disabled)
- **Need Additional Validation** – Enables extended ARP Inspection Validation if any of the following options are enabled. (Default: Disabled)
  - **Source MAC Validation** – Validates the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses.
  - **Destination MAC Validation** – Validates the destination MAC address in the Ethernet header against the target MAC address in the body of ARP responses.
  - **IP Address Validation** – Checks the ARP body for invalid and unexpected IP addresses. Sender IP addresses are checked in all ARP requests and responses, while target IP addresses are checked only in ARP responses.
- **Log Message Number** – The maximum number of entries saved in a log message. (Range: 0-256; Default: 5)
- **Log Message Interval** – The interval at which log messages are sent. (Range: 0-86400 seconds; Default: 1 second)

WEB INTERFACE

To configure global settings for ARP Inspection:

1. Click Security, ARP Inspection, Configuration.
2. Enable ARP inspection globally, enable any of the address validation options, and adjust any of the logging parameters if required.
3. Click Apply.

Figure 95: Configuring Global Settings for ARP Inspection



CONFIGURING VLAN SETTINGS FOR ARP INSPECTION

Use the Security > ARP Inspection > VLAN Configuration page to enable ARP inspection for any VLAN and to specify the ARP ACL to use.

CLI REFERENCES

- "ARP Inspection" on page 649

COMMAND USAGE

ARP Inspection VLAN Filters (ACLs)

- By default, no ARP Inspection ACLs are configured and the feature is disabled.
- ARP Inspection ACLs are configured within the ARP ACL configuration page (see page 234).
- ARP Inspection ACLs can be applied to any configured VLAN.
- ARP Inspection uses the DHCP snooping bindings database for the list of valid IP-to-MAC address bindings. ARP ACLs take precedence over entries in the DHCP snooping bindings database. The switch first compares ARP packets to any specified ARP ACLs.
- If *Static* is specified, ARP packets are only validated against the selected ACL – packets are filtered according to any matching rules, packets not matching any rules are dropped, and the DHCP snooping bindings database check is bypassed.

- If *Static* is not specified, ARP packets are first validated against the selected ACL; if no ACL rules match the packets, then the DHCP snooping bindings database determines their validity.

PARAMETERS

These parameters are displayed:

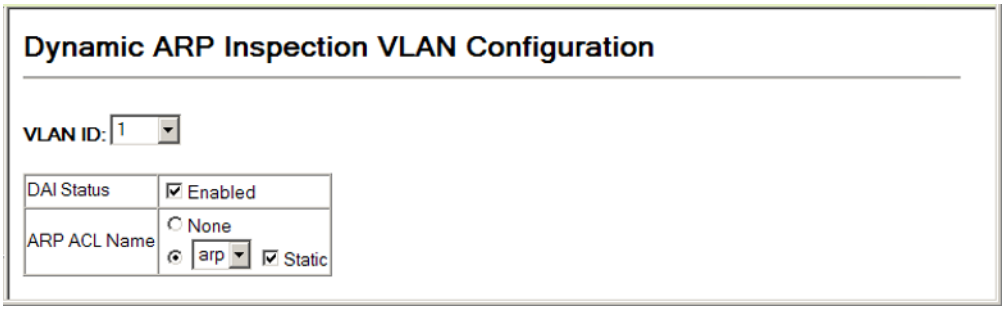
- **VLAN ID** – Selects any configured VLAN. (Default: 1)
- **DAI Status** – Enables Dynamic ARP Inspection for the selected VLAN. (Default: Disabled)
- **ARP ACL Name**
  - *ARP ACL* – Allows selection of any configured ARP ACLs. (Default: None)
  - **Static** – When an ARP ACL is selected, and static mode also selected, the switch only performs ARP Inspection and bypasses validation against the DHCP Snooping Bindings database. When an ARP ACL is selected, but static mode is not selected, the switch first performs ARP Inspection and then validation against the DHCP Snooping Bindings database. (Default: Disabled)

WEB INTERFACE

To configure VLAN settings for ARP Inspection:

1. Click Security, ARP Inspection, VLAN Configuration.
2. Enable ARP inspection for the required VLANs, select an ARP ACL filter to check for configured addresses, and select the Static option to bypass checking the DHCP snooping bindings database if required.
3. Click Apply.

Figure 96: Configuring VLAN Settings for ARP Inspection



CONFIGURING INTERFACE SETTINGS FOR ARP INSPECTION

Use the Security > ARP Inspection > Port Configuration page to specify the ports that require ARP inspection, and to adjust the packet inspection rate.

CLI REFERENCES

- "ARP Inspection" on page 649

PARAMETERS

These parameters are displayed:

- **Port** – Port identifier.
- **Trust Status** – Configures the port as trusted or untrusted. (Default: Untrusted)

  By default, all untrusted ports are subject to ARP packet rate limiting, and all trusted ports are exempt from ARP packet rate limiting.

  Packets arriving on trusted interfaces bypass all ARP Inspection and ARP Inspection Validation checks and will always be forwarded, while those arriving on untrusted interfaces are subject to all configured ARP inspection tests.
- **Rate Limit Status** – If this parameter is enabled, then there is no limit on the number of ARP packets that can be processed by the CPU.
- **Rate Limit** – Sets the maximum number of ARP packets that can be processed by CPU per second on untrusted ports. (Range: 0-2048; Default: 15)

  The switch will drop all ARP packets received on a port which exceeds the configured ARP-packets-per-second rate limit.

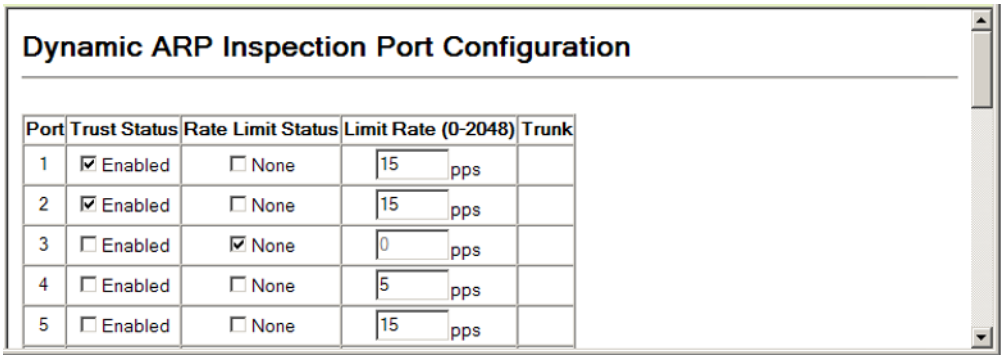
  Setting the rate limit to "0" means that no ARP packets can be forwarded.

WEB INTERFACE

To configure interface settings for ARP Inspection:

1. Click Security, ARP Inspection, Port Configuration.
2. Specify any untrusted ports which require ARP inspection, and adjust the packet inspection rate.
3. Click Apply.

Figure 97: Configuring Interface Settings for ARP Inspection



DISPLAYING THE ARP INSPECTION LOG

Use the Security > ARP Inspection > Log Information page to show information about entries stored in the log, including the associated VLAN, port, and address components.

CLI REFERENCES

- "show ip arp inspection log" on page 657

PARAMETERS

These parameters are displayed:

Table 16: ARP Inspection Log

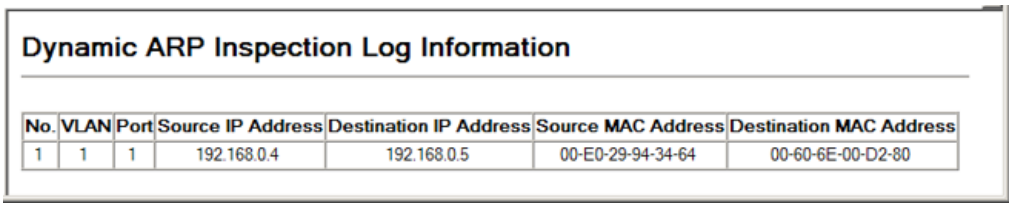
Parameter	Description
No.	Log entry index number.
VLAN	The VLAN where this packet was seen.
Port	The port where this packet was seen.
Src. IP Address	The source IP address in the packet.
Dst. IP Address	The destination IP address in the packet.
Src. MAC Address	The source MAC address in the packet.
Dst. MAC Address	The destination MAC address in the packet.

WEB INTERFACE

To display the ARP Inspection log:

1. Click Security, ARP Inspection.
2. Select Configure Information from the Step list.
3. Select Show Log from the Step list.

Figure 98: Displaying the ARP Inspection Log



DISPLAYING ARP INSPECTION STATISTICS

Use the Security > ARP Inspection > Statistics page to display statistics about the number of ARP packets processed, or dropped for various reasons.

CLI REFERENCES

- "show ip arp inspection statistics" on page 657

PARAMETERS

These parameters are displayed:

Table 17: ARP Inspection Statistics

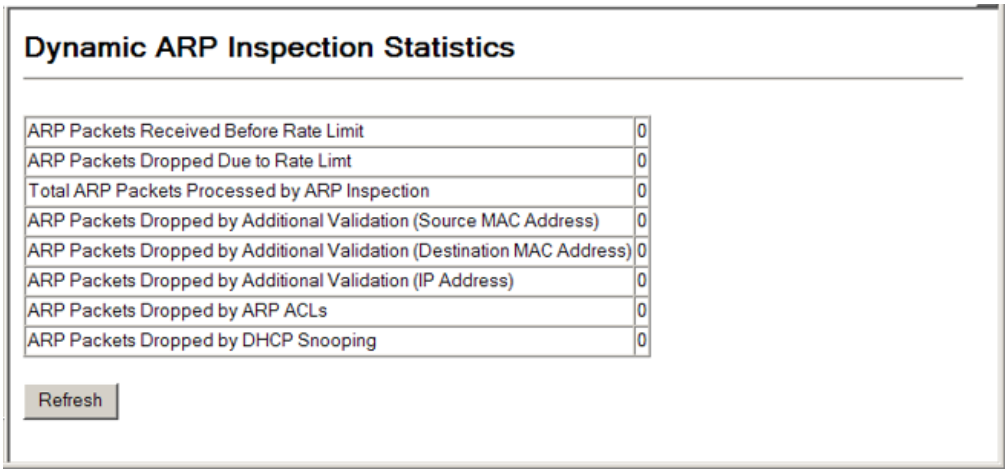
Parameter	Description
ARP Packets Received Before Rate Limit	Count of ARP packets received but not exceeding the ARP Inspection rate limit.
ARP Packets Dropped Due to Rate Limit	Count of ARP packets exceeding (and dropped by) ARP rate limiting.
Total ARP Packets Processed by ARP Inspection	Count of all ARP packets processed by the ARP Inspection engine.
ARP Packets Dropped by Additional Validation (Source MAC Address)	Count of packets that failed the source MAC address test.
ARP Packets Dropped by Additional Validation (Destination MAC Address)	Count of packets that failed the destination MAC address test.
ARP Packets Dropped by Additional Validation (IP Address)	Count of ARP packets that failed the IP address test.
ARP Packets Dropped by ARP ACLs	Count of ARP packets that failed validation against ARP ACL rules.
ARP Packets Dropped by DHCP Snooping	Count of packets that failed validation against the DHCP Snooping Binding database.

WEB INTERFACE

To display statistics for ARP Inspection:

1. Click Security, ARP Inspection, Statistics.

Figure 99: Displaying Statistics for ARP Inspection



FILTERING IP ADDRESSES FOR MANAGEMENT ACCESS

Use the Security > IP Filter page to create a list of up to 16 IP addresses or IP address groups that are allowed management access to the switch through the web interface, SNMP, or Telnet.

CLI REFERENCES

- "Management IP Filter" on page 604

COMMAND USAGE

- The management interfaces are open to all IP addresses by default. Once you add an entry to a filter list, access to that interface is restricted to the specified addresses.
- If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- IP address can be configured for SNMP, web and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.
- When entering addresses for the same group (i.e., SNMP, web or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.

- You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.
- You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

PARAMETERS

These parameters are displayed:

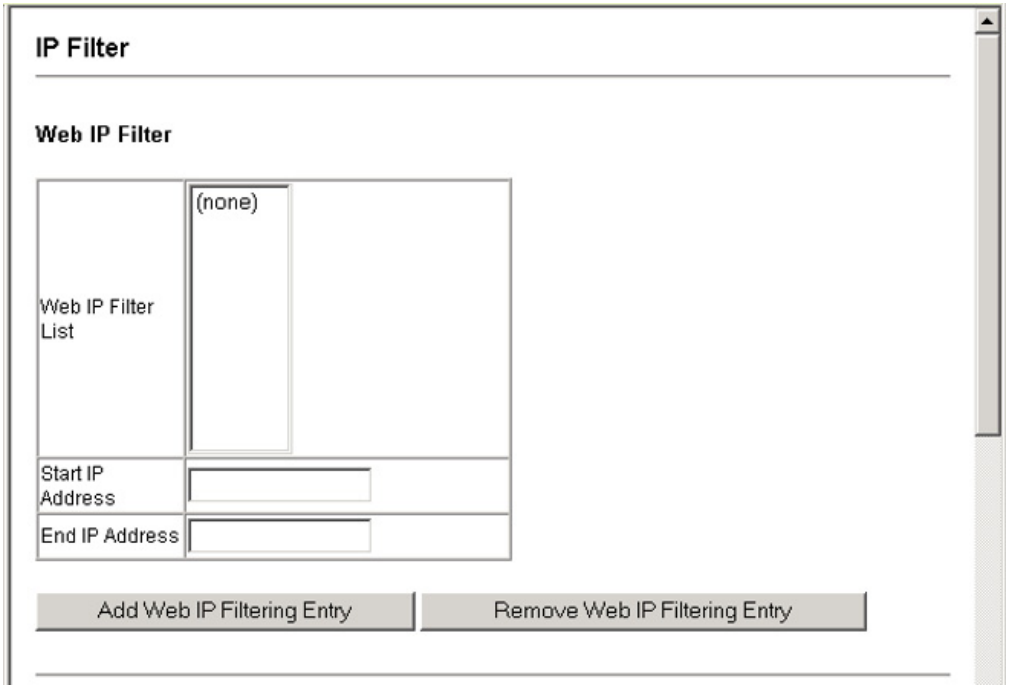
- **Web IP Filter** – Configures IP address(es) for the web group.
- **SNMP IP Filter** – Configures IP address(es) for the SNMP group.
- **Telnet IP Filter** – Configures IP address(es) for the Telnet group.
- **Start IP Address** – A single IP address, or the starting address of a range.
- **End IP Address** – The end address of a range.
- **Add/Remove Filtering Entry** – Adds/removes an IP address from the list.

WEB INTERFACE

To create a list of IP addresses authorized for management access:

1. Click Security, IP Filter.
2. Enter the IP addresses or range of addresses that are allowed management access to an interface.
3. Click Add IP Filtering Entry.

Figure 100: Creating an IP Address Filter for Management Access



DHCP SNOOPING

The addresses assigned to DHCP clients on insecure ports can be carefully controlled using the dynamic bindings registered with DHCP Snooping (or using the static bindings configured with IP Source Guard). DHCP snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port.

COMMAND USAGE

DHCP Snooping Process

- Network traffic may be disrupted when malicious DHCP messages are received from an outside source. DHCP snooping is used to filter DHCP messages received on a non-secure interface from outside the network or fire wall. When DHCP snooping is enabled globally and enabled on a VLAN interface, DHCP messages received on an untrusted interface from a device not listed in the DHCP snooping table will be dropped.

- Table entries are only learned for trusted interfaces. An entry is added or removed dynamically to the DHCP snooping table when a client receives or releases an IP address from a DHCP server. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier.

- The rate limit for the number of DHCP messages that can be processed by the switch is 100 packets per second. Any DHCP packets in excess of this limit are dropped.

- When DHCP snooping is enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.
- Filtering rules are implemented as follows:
  - If the global DHCP snooping is disabled, all DHCP packets are forwarded.
  - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a *trusted* port. If the received packet is a DHCP ACK message, a dynamic DHCP snooping entry is also added to the binding table.
  - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is *not trusted*, it is processed as follows:
    - If the DHCP packet is a reply packet from a DHCP server (including OFFER, ACK or NAK messages), the packet is dropped.
    - If the DHCP packet is from a client, such as a DECLINE or RELEASE message, the switch forwards the packet only if the corresponding entry is found in the binding table.
    - If the DHCP packet is from a client, such as a DISCOVER, REQUEST, INFORM, DECLINE or RELEASE message, the packet is forwarded if MAC address verification is disabled. However, if MAC address verification is enabled, then the packet will only be forwarded if the client's hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.
    - If the DHCP packet is not a recognizable type, it is dropped.
  - If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.
  - If a DHCP packet is from server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.
  - If the DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.
  - *Additional considerations when the switch itself is a DHCP client* – The port(s) through which the switch submits a client request to the DHCP server must be configured as trusted. Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCP server. Also, when the switch sends out DHCP client packets for itself, no filtering takes place. However, when the switch receives any messages from a DHCP server, any packets received from untrusted ports are dropped.

DHCP SNOOPING CONFIGURATION

Use the DHCP Snooping > Configuration page to enable DHCP Snooping globally on the switch, or to configure MAC Address Verification.

CLI REFERENCES

- "DHCP Snooping" on page 635

PARAMETERS

These parameters are displayed:

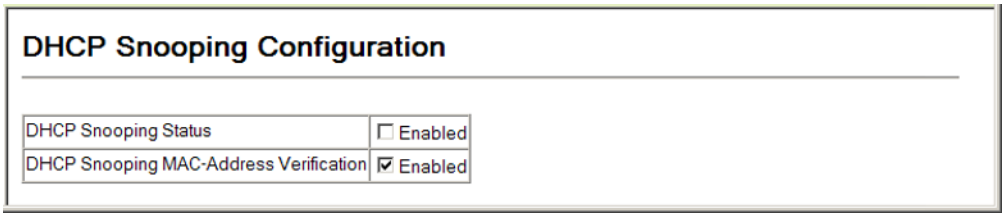
- **DHCP Snooping Status –** Enables DHCP snooping globally. (Default: Disabled)
- **DHCP Snooping MAC-Address Verification** – Enables or disables MAC address verification. If the source MAC address in the Ethernet header of the packet is not same as the client's hardware address in the DHCP packet, the packet is dropped. (Default: Enabled)

WEB INTERFACE

To configure global settings for DHCP Snooping:

1. Click DHCP Snooping, Configuration.
2. Set the status for the global DHCP snooping process, and enable or disable MAC-address verification as required.
3. Click Apply

Figure 101: Configuring Global Settings for DHCP Snooping



DHCP SNOOPING VLAN CONFIGURATION

Use the DHCP Snooping > VLAN Configuration page to enable or disable DHCP snooping on specific VLANs.

CLI REFERENCES

- "ip dhcp snooping vlan" on page 640

COMMAND USAGE

- When DHCP snooping is enabled globally on the switch, and enabled on the specified VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN.
- When the DHCP snooping is globally disabled, DHCP snooping can still be configured for specific VLANs, but the changes will not take effect until DHCP snooping is globally re-enabled.

- When DHCP snooping is globally enabled, and DHCP snooping is then disabled on a VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.

PARAMETERS

These parameters are displayed:

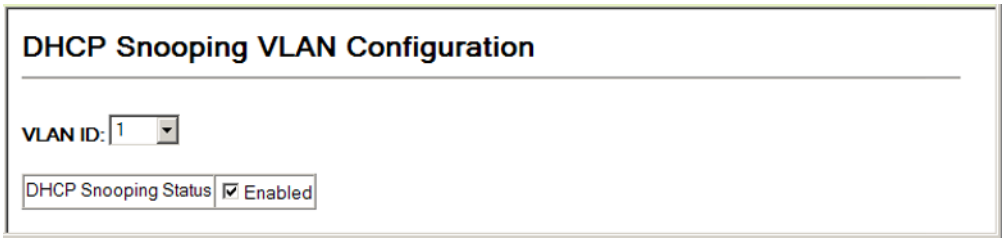
- **VLAN** – ID of a configured VLAN. (Range: 1-4094)
- **DHCP Snooping Status** – Enables or disables DHCP snooping for the selected VLAN. When DHCP snooping is enabled globally on the switch, and enabled on the specified VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN. (Default: Disabled)

WEB INTERFACE

To configure global settings for DHCP Snooping:

1. Click DHCP Snooping, VLAN Configuration.
2. Enable DHCP Snooping on any existing VLAN.
3. Click Apply

Figure 102: Configuring DHCP Snooping on a VLAN



DHCP SNOOPING INFORMATION OPTION CONFIGURATION

Use the DHCP Snooping > Information Option Configuration page to configure DHCP Snooping Option 82.

CLI REFERENCES

- "ip dhcp snooping information option" on page 638
- "ip dhcp snooping information policy" on page 639

COMMAND USAGE

- DHCP provides a relay mechanism for sending information about its DHCP clients or the relay agent itself to the DHCP server. Also known as DHCP Option 82, it allows compatible DHCP servers to use the information when assigning IP addresses, or to set other services or policies for clients. It is also an effective tool in preventing malicious network attacks from attached clients on DHCP services, such as IP Spoofing, Client Identifier Spoofing, MAC Address Spoofing, and Address Exhaustion.

- DHCP Snooping must be enabled for Option 82 information to be inserted into request packets.

- When the DHCP Snooping Information Option 82 is enabled, the requesting client (or an intermediate relay agent that has used the information fields to describe itself) can be identified in the DHCP request packets forwarded by the switch and in reply packets sent back from the DHCP server. This information may specify the MAC address or IP address of the requesting device (that is, the switch in this context).

  By default, the switch also fills in the Option 82 circuit-id field with information indicating the local interface over which the switch received the DHCP client request, including the port and VLAN ID. This allows DHCP client-server exchange messages to be forwarded between the server and client without having to flood them to the entire VLAN.

- If DHCP Snooping Information Option 82 is enabled on the switch, information may be inserted into a DHCP request packet received over any VLAN (depending on DHCP snooping filtering rules). The information inserted into the relayed packets includes the circuit-id and remote-id, as well as the gateway Internet address.

- When the switch receives DHCP packets from clients that already include DHCP Option 82 information, the switch can be configured to set the action policy for these packets. The switch can either drop the DHCP packets, keep the existing information, or replace it with the switch's relay information.

PARAMETERS

These parameters are displayed:

- **DHCP Snooping Information Option Status** – Enables or disables DHCP Option 82 information relay. (Default: Disabled)

- **DHCP Snooping Information Option Policy** – Specifies how to handle DHCP client request packets which already contain Option 82 information.

  - **Drop** – Drops the client's request packet instead of relaying it.

  - **Keep** – Retains the Option 82 information in the client request, and forwards the packets to trusted ports.

  - **Replace** – Replaces the Option 82 information circuit-id and remote-id fields in the client's request with information about the relay agent itself, inserts the relay agent's address (when DHCP snooping is enabled), and forwards the packets to trusted ports. (This is the default policy.)

WEB INTERFACE

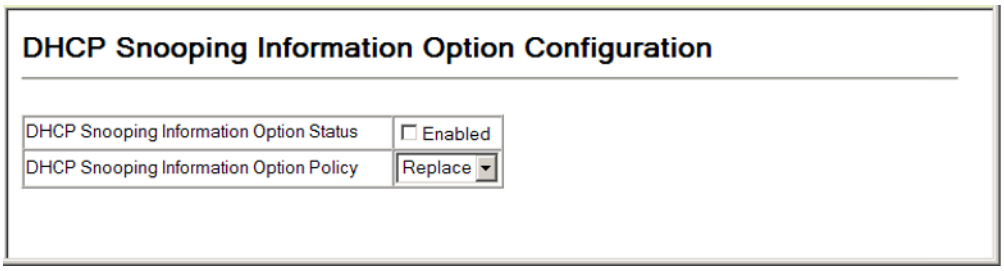
To configure DHCP Snooping Option 82:

1. Click DHCP Snooping, Information Option Configuration.

2. Select the required options for the DHCP information option.

3. Click Apply

Figure 103: Configuring DHCP Snooping Information Option



CONFIGURING PORTS FOR DHCP SNOOPING

Use the DHCP Snooping > Port Configuration page to configure switch ports as trusted or untrusted.

CLI REFERENCES

- "ip dhcp snooping trust" on page 641

COMMAND USAGE

- A trusted interface is an interface that is configured to receive only messages from within the network. An untrusted interface is an interface that is configured to receive messages from outside the network or fire wall.

- When DHCP snooping is enabled both globally and on a VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN.

- When an untrusted port is changed to a trusted port, all the dynamic DHCP snooping bindings associated with this port are removed.

- Set all ports connected to DHCP servers within the local network or fire wall to trusted state. Set all other ports outside the local network or fire wall to untrusted state.

PARAMETERS

These parameters are displayed:

- **Trust Status** – Enables or disables a port as trusted. (Default: Disabled)

WEB INTERFACE

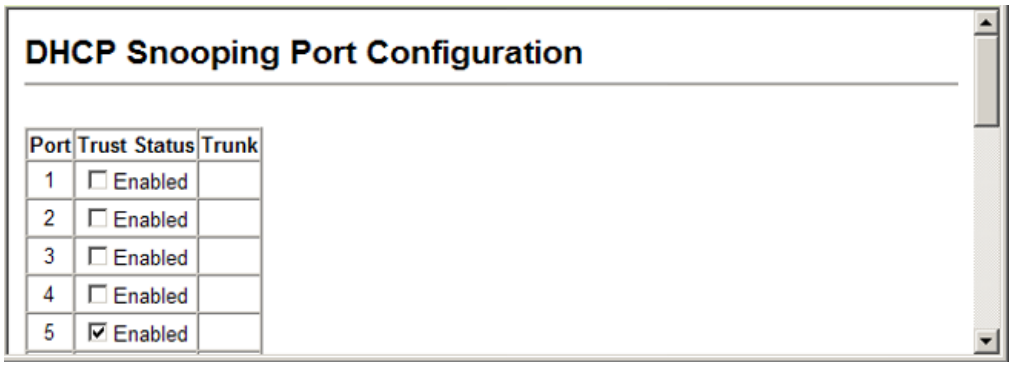
To configure global settings for DHCP Snooping:

1. Click DHCP Snooping, Port Configuration.

2. Set any ports within the local network or firewall to trusted.

3. Click Apply

Figure 104: Configuring the Port Mode for DHCP Snooping



DISPLAYING DHCP SNOOPING BINDING INFORMATION

Use the DHCP Snooping > Binding Information page to display entries in the binding table.

CLI REFERENCES

- "show ip dhcp snooping binding" on page 643

PARAMETERS

These parameters are displayed:

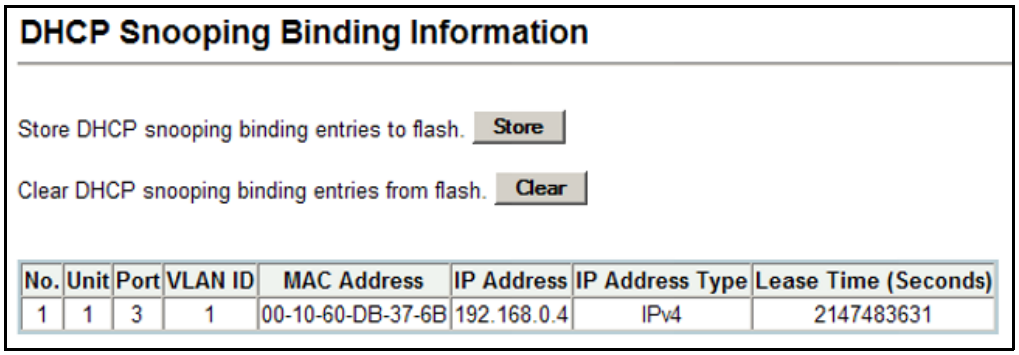
- **Store DHCP Snooping binding entries to flash** – Writes all dynamically learned snooping entries to flash memory. This function can be used to store the currently learned dynamic DHCP snooping entries to flash memory. These entries will be restored to the snooping table when the switch is reset. However, note that the lease time shown for a dynamic entry that has been restored from flash memory will no longer be valid.
- **Clear DHCP Snooping binding entries from flash** – Removes all dynamically learned snooping entries from flash memory.
- **No.** – Entry number for DHCP snooping binding information.
- **Unit** – Stack unit.
- **Port** – Port to which this entry is bound.
- **VLAN ID** – VLAN to which this entry is bound.
- **MAC Address** – Physical address associated with the entry.
- **IP Address** – IP address corresponding to the client.
- **IP Address Type** – Indicates an IPv4 or IPv6 address type.
- **Lease Time** (Seconds) – The time for which this IP address is leased to the client.

WEB INTERFACE

To display the binding table for DHCP Snooping:

1. Click DHCP Snooping, Binding Information.
2. Use the Store or Clear function if required.

Figure 105: Displaying the Binding Table for DHCP Snooping



IP SOURCE GUARD

IP Source Guard is a security feature that filters IP traffic on network interfaces based on manually configured entries in the IP Source Guard table, or dynamic entries in the DHCP Snooping table when enabled (see "DHCP Snooping"). IP source guard can be used to prevent traffic attacks caused when a host tries to use the IP address of a neighbor to access the network. This section describes commands used to configure IP Source Guard.

CONFIGURING PORTS FOR IP SOURCE GUARD

Use the IP Source Guard > Port Configuration page to set the filtering type based on source IP address, or source IP address and MAC address pairs.

IP Source Guard is used to filter traffic on an insecure port which receives messages from outside the network or fire wall, and therefore may be subject to traffic attacks caused by a host trying to use the IP address of a neighbor.

CLI REFERENCES

- "ip source-guard" on page 646

COMMAND USAGE

- Setting source guard mode to SIP (Source IP) or SIP-MAC (Source IP and MAC) enables this function on the selected port. Use the SIP option to check the VLAN ID, source IP address, and port number against all entries in the binding table. Use the SIP-MAC option to check these same parameters, plus the source MAC address. If no matching entry is found, the packet is dropped.

NOTE: Multicast addresses cannot be used by IP Source Guard.

- When enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping (see "DHCP Snooping"), or static addresses configured in the source guard binding table.
- If IP source guard is enabled, an inbound packet's IP address (SIP option) or both its IP address and corresponding MAC address (SIP-MAC option) will be checked against the binding table. If no matching entry is found, the packet will be dropped.
- Filtering rules are implemented as follows:
  - If DHCP snooping is disabled (see page 250), IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the SIP-MAC option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, the packet will be forwarded.
  - If DHCP snooping is enabled, IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the SIP-MAC option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, or dynamic DHCP snooping binding, the packet will be forwarded.
  - If IP source guard if enabled on an interface for which IP source bindings have not yet been configured (neither by static configuration in the IP source guard binding table nor dynamically learned from DHCP snooping), the switch will drop all IP traffic on that port, except for DHCP packets.

PARAMETERS

These parameters are displayed:

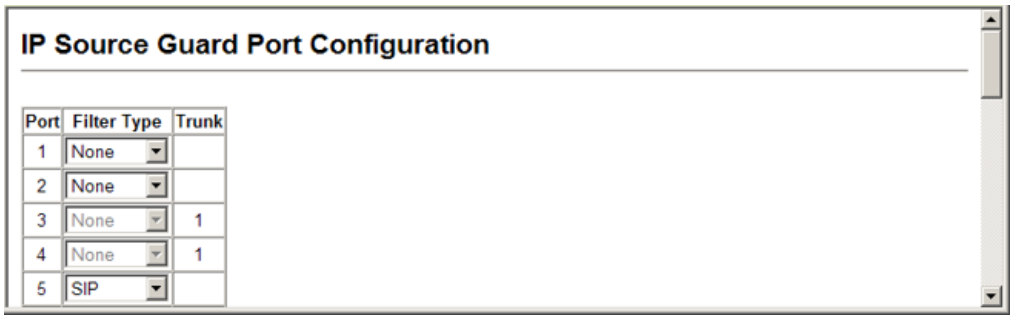
- **Filter Type** – Configures the switch to filter inbound traffic based source IP address, or source IP address and corresponding MAC address. (Default: None)
  - **None** – Disables IP source guard filtering on the port.
  - **SIP** – Enables traffic filtering based on IP addresses stored in the binding table.
  - **SIP-MAC** – Enables traffic filtering based on IP addresses and corresponding MAC addresses stored in the binding table.

WEB INTERFACE

To set the IP Source Guard filter for ports:

1. Click IP Source Guard, Port Configuration.
2. Set the required filtering type for each port.
3. Click Apply

Figure 106: Setting the Filter Type for IP Source Guard



CONFIGURING STATIC BINDINGS FOR IP SOURCE GUARD

Use the IP Source Guard > Static Configuration page to bind a static address to a port. Table entries include a MAC address, IP address, lease time, entry type (Static, Dynamic), VLAN identifier, and port identifier. All static entries are configured with an infinite lease time, which is indicated with a value of zero in the table.

CLI REFERENCES

- "ip source-guard binding" on page 644

COMMAND USAGE

- Static addresses entered in the source guard binding table are automatically configured with an infinite lease time. Dynamic entries learned via DHCP snooping are configured by the DHCP server itself.
- Static bindings are processed as follows:
  - If there is no entry with the same VLAN ID and MAC address, a new entry is added to the binding table using the type "static IP source guard binding."
  - If there is an entry with the same VLAN ID and MAC address, and the type of entry is static IP source guard binding, then the new entry will replace the old one.
  - If there is an entry with the same VLAN ID and MAC address, and the type of the entry is dynamic DHCP snooping binding, then the new entry will replace the old one and the entry type will be changed to static IP source guard binding.
  - Only unicast addresses are accepted for static bindings.

PARAMETERS

These parameters are displayed:

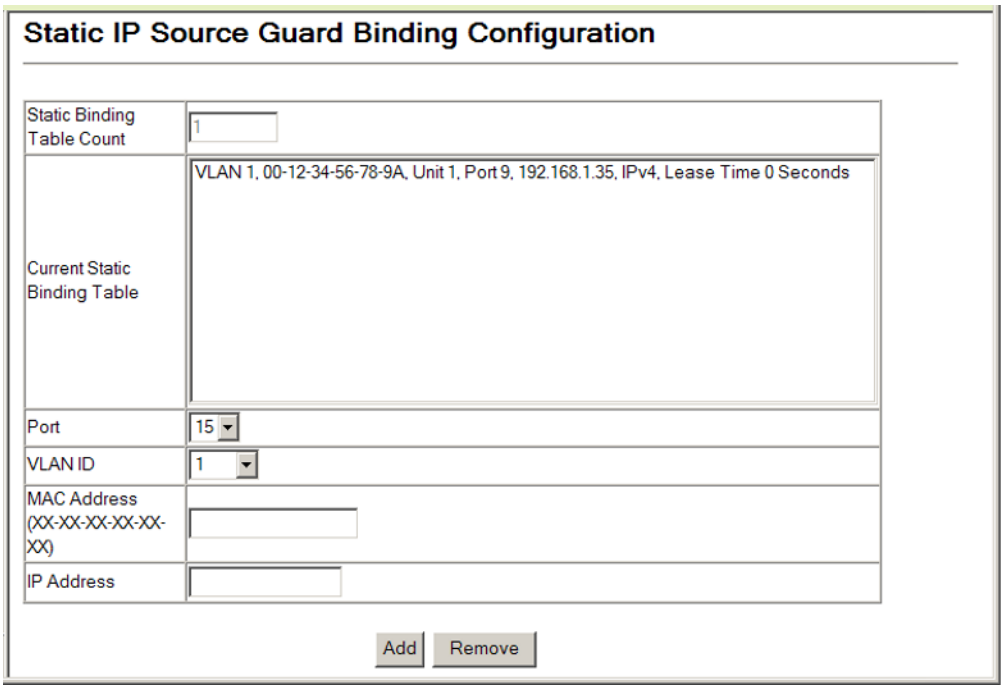
- **Static Binding Table Counts** – The total number of static entries in the table.
- **Current Static Binding Table** – The list of current static entries in the table.
- **Port** – The port to which a static entry is bound.
- **VLAN ID** – ID of a configured VLAN (Range: 1-4094)
- **MAC Address** – A valid unicast MAC address.
- **IP Address** – A valid unicast IP address, including classful types A, B or C.

WEB INTERFACE

To configure static bindings for IP Source Guard:

1. Click IP Source Guard, Static Configuration.
2. Enter the required bindings for each port.
3. Click Add.

Figure 107: Configuring Static Bindings for IP Source Guard



DISPLAYING INFORMATION FOR DYNAMIC IP SOURCE GUARD BINDINGS

Use the IP Source Guard > Dynamic Binding page to display the source-guard binding table for a selected interface.

CLI REFERENCES

- "show ip source-guard binding" on page 648

PARAMETERS

These parameters are displayed:

Query by

- **Port** – A port on this switch.
- **VLAN** – ID of a configured VLAN (Range: 1-4093)
- **MAC Address** – A valid unicast MAC address.
- **IP Address** – A valid unicast IP address, including classful types A, B or C.

Dynamic Binding List

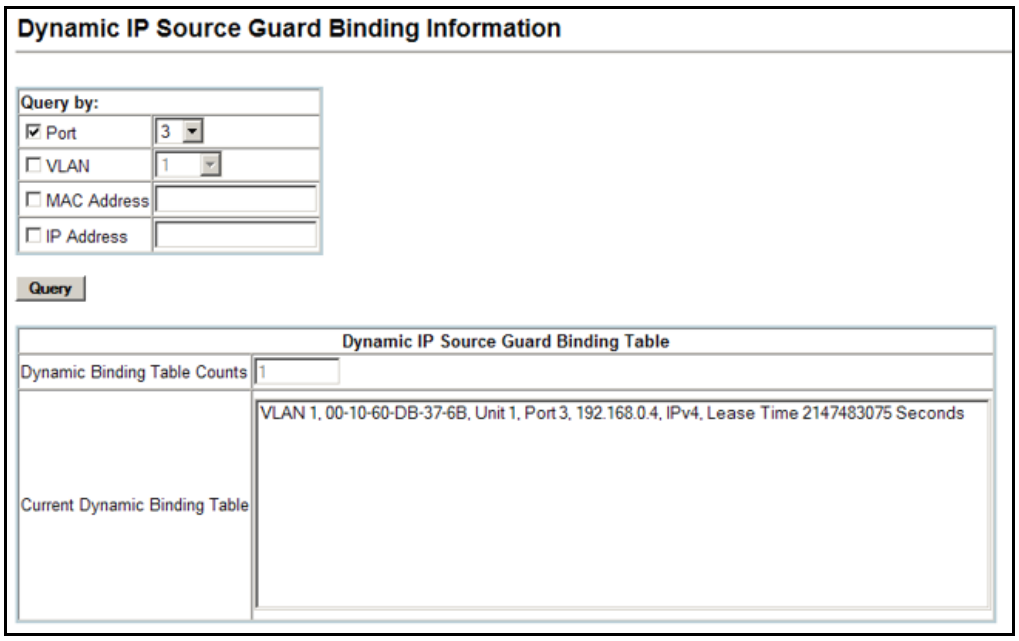
- **VLAN** – VLAN to which this entry is bound.
- **MAC Address** – Physical address associated with the entry.
- **Unit** – Stack unit.
- **Port** – Port to which this entry is bound.
- **IP Address** – IP address corresponding to the client.
- **IP Address Type** – Indicates an IPv4 or IPv6 address type.
- **Lease Time** – The time for which this IP address is leased to the client.

WEB INTERFACE

To display the binding table for IP Source Guard:

1. Click IP Source Guard, Dynamic Information.
2. Mark the search criteria, and enter the required values.
3. Click Query

Figure 108: Showing the IP Source Guard Binding Table



8 INTERFACE CONFIGURATION

This chapter describes the following topics:

- Port Configuration – Configures connection settings, including auto-negotiation, or manual setting of speed, duplex mode, and flow control.
- Trunk Configuration – Configures static or dynamic trunks.
- Storm Control Configuration – Controls the maximum amount of traffic caused by broadcast, multicast or unknown unicast storms that will be forwarded by the switch.
- Mirror Configuration – Mirrors traffic from a source port to a target port.
- Rate Limiting – Limits the traffic rate for ingress or egress ports.
- VLAN Trunking – Configures a tunnel across one or more intermediate switches which pass traffic for VLAN groups to which they do not belong.
- Cable Test – Tests the cable attached to a port.
- Displaying Statistics – Shows Interface, Etherlike, and RMON port statistics in table or chart form.

PORT CONFIGURATION

This section describes how to configure port connections, mirror traffic from one port to another, and run cable diagnostics.

DISPLAYING CONNECTION STATUS

Use the Port > Port Information or Trunk Information page to display the current connection status, including link state, speed/duplex mode, flow control, and auto-negotiation.

CLI REFERENCES

- "show interfaces status" on page 694

PARAMETERS

These parameters are displayed:

- **Port** – Port identifier.
- **Name** – Interface label.

- **Type** – Indicates the port type. (100Base-TX, 1000Base-T, 100Base SFP or 1000Base SFP)
- **Admin Status** – Shows if the port is enabled or disabled.
- **Oper Status** – Indicates if the link is Up or Down.
- **Speed Duplex Status** – Shows the current speed and duplex mode.
- **Flow Control Status** – Shows if flow control is enabled or disabled.
- **Autonegotiation** – Shows if auto-negotiation is enabled or disabled.
- **Media Type**[5] – Media type used. (Options: Copper-Forced, SFP-Forced, or SFP-Preferred-Auto; Default: SFP-Preferred-Auto)
- **Trunk Member**[6] – Shows if port is a trunk member.
- **Creation**[6] – Shows if a trunk is manually configured or dynamically set via LACP.

WEB INTERFACE

To display port connection parameters:

1. Click Port, Port Information.

Figure 109: Displaying Port Information

Port Information

Port	Name	Type	Admin Status	Oper Status	Speed Duplex Status	Flow Control Status	Autonegotiation	Media Type	Trunk Member
1		100Base-TX	Enabled	Up	100full	None	Enabled	None	
2		100Base-TX	Enabled	Down	10half	None	Enabled	None	
3		100Base-TX	Enabled	Down	10half	None	Enabled	None	
4		100Base-TX	Enabled	Down	10half	None	Enabled	None	
5		100Base-TX	Enabled	Down	10half	None	Enabled	None	
6		100Base-TX	Enabled	Down	10half	None	Enabled	None	
7		100Base-TX	Enabled	Down	10half	None	Enabled	None	
8		100Base-TX	Enabled	Down	10half	None	Enabled	None	

CONFIGURING INTERFACE CONNECTIONS

Use the Port > Port Configuration or Trunk Configuration page to enable/disable an interface, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed, duplex mode, and flow control.

CLI REFERENCES

- "Interface Commands" on page 681

5. Port information only.
6. Trunk information only.

COMMAND USAGE

- Auto-negotiation must be disabled before you can configure or force the interface to use the Speed/Duplex mode or Flow Control options.
- When using auto-negotiation, the optimal settings will be negotiated between the link partners based on their advertised capabilities. To set the speed, duplex mode, or flow control under auto-negotiation, the required operation modes must be specified in the capabilities list for an interface.
- The 1000BASE-T standard does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk. If not used, the success of the link process cannot be guaranteed when connecting to other types of switches. However, this switch does provide a means of safely forcing a link to operate at 1000 Mbps, full-duplex using the Giga Phy Mode attribute described below.

PARAMETERS

These parameters are displayed:

- **Name** – Allows you to label an interface. (Range: 1-64 characters)
- **Port** – Port identifier. (Range: 1-28/52)
- **Admin** – Allows you to manually disable an interface. You can disable an interface due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also disable an interface for security reasons.
- **Speed/Duplex** – Allows you to manually set the port speed and duplex mode. (i.e., with auto-negotiation disabled)
- **Flow Control** – Allows automatic or manual selection of flow control.
- **Giga PHY Mode** – Forces two connected ports into a master/slave configuration to enable 1000BASE-T full duplex for Gigabit ports 25-28/49-52. The following options are supported:
  - **Master** - Sets the selected port as master.
  - **Slave** - Sets the selected port as slave.
  - **Auto Prefer Master** - Uses master mode as the initial configuration setting regardless of the mode configured at the other end of the link.
  - **Auto Prefer Slave** - Uses slave mode as the initial configuration regardless of the mode configured at the other end of the link.

  To force 1000full operation requires the ports at both ends of a link to establish their role in the connection process as a master or slave. Before using this feature, auto-negotiation must first be disabled, and the Speed/Duplex attribute set to 1000full. Then select compatible Giga PHY modes at both ends of the link. Note that using one of the

preferred modes ensures that the ports at both ends of a link will eventually cooperate to establish a valid master-slave relationship.

- **Autonegotiation** (Port Capabilities) – Allows auto-negotiation to be enabled/disabled. When auto-negotiation is enabled, you need to specify the capabilities to be advertised. When auto-negotiation is disabled, you can force the settings for speed, mode, and flow control.The following capabilities are supported.
  - **10half** - Supports 10 Mbps half-duplex operation
  - **10full** - Supports 10 Mbps full-duplex operation
  - **100half** - Supports 100 Mbps half-duplex operation
  - **100full** - Supports 100 Mbps full-duplex operation
  - **1000full** (Gigabit ports only) - Supports 1000 Mbps full-duplex operation
  - **Sym** (Gigabit only) - Check this item to transmit and receive pause frames.
  - **FC** - Flow control can eliminate frame loss by "blocking" traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3-2005 (formally IEEE 802.3x) for full-duplex operation.

    Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.

    (Default: Autonegotiation enabled; Advertised capabilities for 100Base-TX – 10half, 10full, 100half, 100full; 1000BASE-T – 10half, 10full, 100half, 100full, 1000full; 1000Base-SX/LX/LH – 1000full)

- **Media Type** – Configures the forced/preferred port type to use for the combination ports (Ports 25-26/49-52).
  - **Copper-Forced** - Always uses the built-in RJ-45 port.
  - **SFP-Forced** - Always uses the SFP port (even if a module is not installed).
  - **SFP-Preferred-Auto** - Uses SFP port if both combination types are functioning and the SFP port has a valid link. (This is the default.)

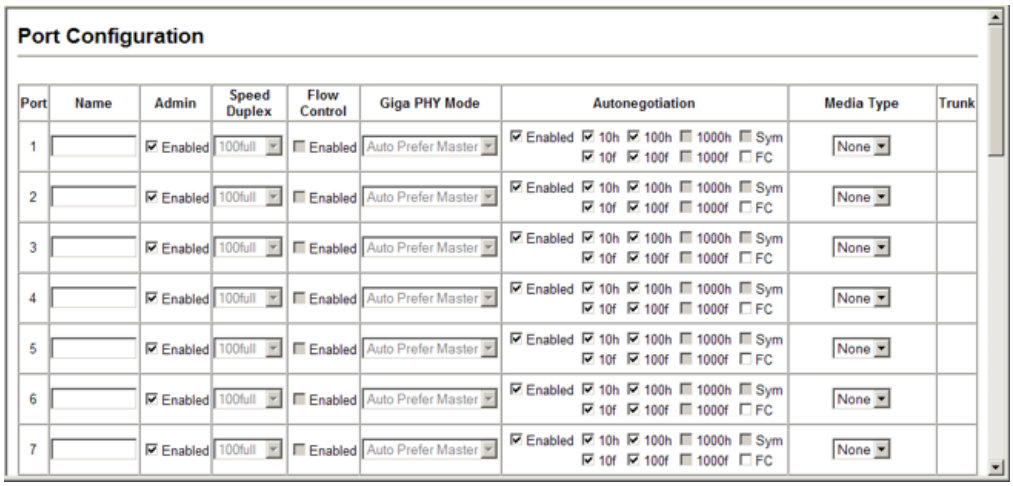
- **Trunk** – Indicates if a port is a member of a trunk. To create trunks and select port members, see "Trunk Configuration."

WEB INTERFACE

To configure port connection parameters:

1. Click Port, Port Configuration.
2. Modify the required interface settings.
3. Click Apply.

Figure 110: Configuring Interface Connections



TRUNK CONFIGURATION

This section describes how to configure static and dynamic trunks.

You can create multiple links between devices that work as one virtual, aggregate link. A port trunk offers a dramatic increase in bandwidth for network segments where bottlenecks exist, as well as providing a fault-tolerant link between two devices. You can create up to 8 trunks at a time on the switch.

The switch supports both static trunking and dynamic Link Aggregation Control Protocol (LACP). Static trunks have to be manually configured at both ends of the link, and the switches must comply with the Cisco EtherChannel standard. On the other hand, LACP configured ports can automatically negotiate a trunked link with LACP-configured ports on another device. You can configure any number of ports on the switch as LACP, as long as they are not already configured as part of a static trunk. If ports on another device are also configured as LACP, the switch and the other device will negotiate a trunk link between them. If an LACP trunk consists of more than eight ports, all other ports will be placed in standby mode. Should one link in the trunk fail, one of the standby ports will automatically be activated to replace it.

COMMAND USAGE

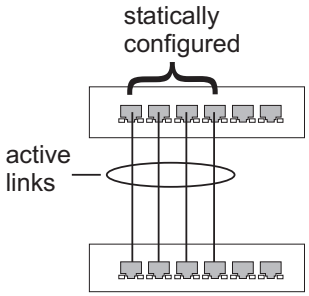
Besides balancing the load across each port in the trunk, the other ports provide redundancy by taking over the load if a port in the trunk fails. However, before making any physical connections between devices, use the web interface or CLI to specify the trunk on the devices at both ends. When using a port trunk, take note of the following points:

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- You can create up to 8 trunks on a switch, with up to eight ports per trunk.
- The ports at both ends of a connection must be configured as trunk ports.
- When configuring static trunks on switches of different types, they must be compatible with the Cisco EtherChannel standard.
- The ports at both ends of a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- Any of the Gigabit ports on the front panel can be trunked together, including ports of different media types.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- STP, VLAN, and IGMP settings can only be made for the entire trunk.

CONFIGURING A STATIC TRUNK

Use the Port > Trunk Membership page to create a trunk, assign member ports, and configure the connection parameters.

Figure 111: Configuring Static Trunks



CLI REFERENCES

- "Link Aggregation Commands" on page 701
- "Interface Commands" on page 681

COMMAND USAGE

- When configuring static trunks, you may not be able to link switches of different types, depending on the manufacturer's implementation. However, note that the static trunks on this switch are Cisco EtherChannel compatible.

- To avoid creating a loop in the network, be sure you add a static trunk via the configuration interface before connecting the ports, and also disconnect the ports before removing a static trunk via the configuration interface.

PARAMETERS

These parameters are displayed:

- **Current** – Shows configured trunks (Trunk ID, Unit, Port).

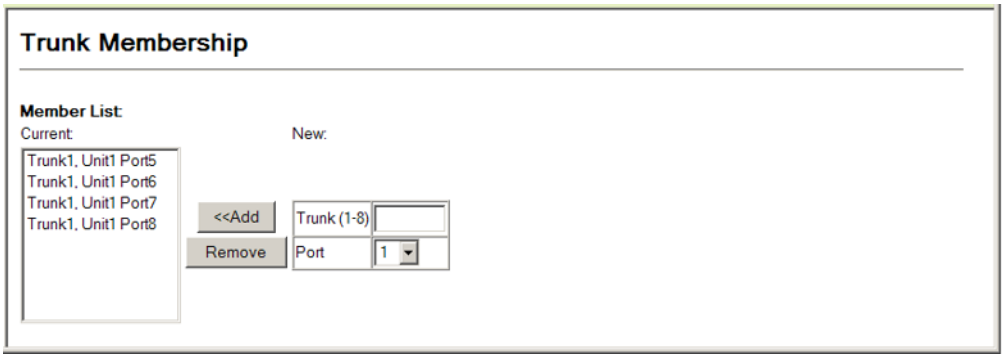
- **New** – Includes entry fields for creating new trunks.
  - **Trunk** – Trunk identifier. (Range: 1-8)
  - **Port** – Port identifier. (Range: 1-28/52)

WEB INTERFACE

To create a static trunk:

1. Click Port, Trunk Member.
2. Enter a trunk identifier.
3. Select any of the switch ports from the scroll-down port list.
4. Click Add.

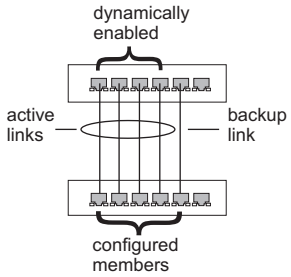
Figure 112: Creating Static Trunks



ENABLING LACP ON SELECTED PORTS

Use the Interface > Trunk > Configuration page to enable LACP on a port.

Figure 113: Configuring Dynamic Trunks



CLI REFERENCES

- "lacp" on page 703

COMMAND USAGE

- To avoid creating a loop in the network, be sure you enable LACP before connecting the ports, and also disconnect the ports before disabling LACP.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- A trunk formed with another switch using LACP will automatically be assigned the next available trunk ID.
- If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.
- All ports on both ends of an LACP trunk must be configured for full duplex, and auto-negotiation.
- Trunks dynamically established through LACP will also be shown in the Member List on the Trunk Membership menu (see page 266).

PARAMETERS

These parameters are displayed:

- **Current** – Shows LACP-enabled ports. (Unit, Port).
- **New** – Shows ports not yet enabled for LACP.
  - **Port** – Port identifier. (Range: 1-28/52)

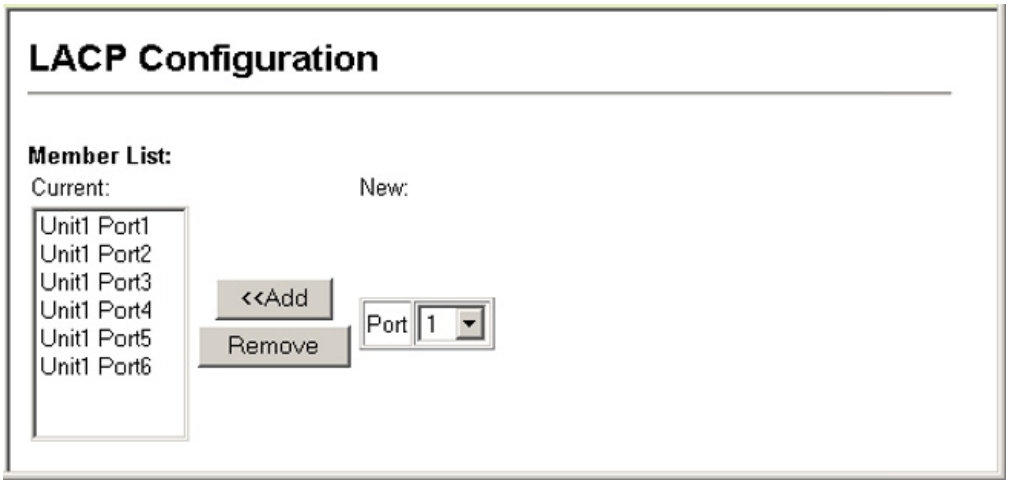
WEB INTERFACE

To enable LACP for a port:

1. Click Port, LACP, Configuration.
2. Select any of the switch ports from the scroll-down port list.

3. Click Apply.

Figure 114: Enabling LACP on a Port



CONFIGURING PARAMETERS FOR LACP GROUP MEMBERS

Use the Port > LACP > Dynamic Aggregation Port page to set the administrative key for a group member, and configure protocol parameters for local and partner ports.

CLI REFERENCES

- "Link Aggregation Commands" on page 701

COMMAND USAGE

Dynamically Creating a Port Channel –

Ports assigned to a common port channel must meet the following criteria:

- Ports must have the same LACP System Priority.
- Ports must have the same LACP port Admin Key.
- Ports are only allowed to join the same Link Aggregation Group (LAG) if (1) the LACP port system priority matches, (2) the LACP port admin key matches, and (3) the LAG admin key matches (if configured). However, if the LAG admin key is set, then the port admin key must be set to the same value for a port to be allowed to join that group.

NOTE: If the LAG admin key is not set when a channel group is formed (i.e., it has a null value of 0), the operational value of this key is set to the same value as the port admin key used by the interfaces that joined the group.

PARAMETERS

These parameters are displayed:

Configure Aggregation Port - Actor/Partner

- **Port** – Port number. (Range: 1-28/52)
- **System Priority** – LACP system priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535; Default: 32768)

  Ports must be configured with the same system priority to join the same LAG.

  System priority is combined with the switch's MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.
- **Admin Key** – The LACP administration key must be set to the same value for ports that belong to the same LAG. (Range: 0-65535; Default: 1)

  By default, the Actor Admin Key is determined by port's link speed, and copied to the Oper Key. The Partner Admin Key is assigned zero, and the Oper Key is set based upon LACP PDUs received from the Partner.
- **Port Priority** – If a link goes down, LACP port priority is used to select a backup link. (Range: 0-65535; Default: 32768)

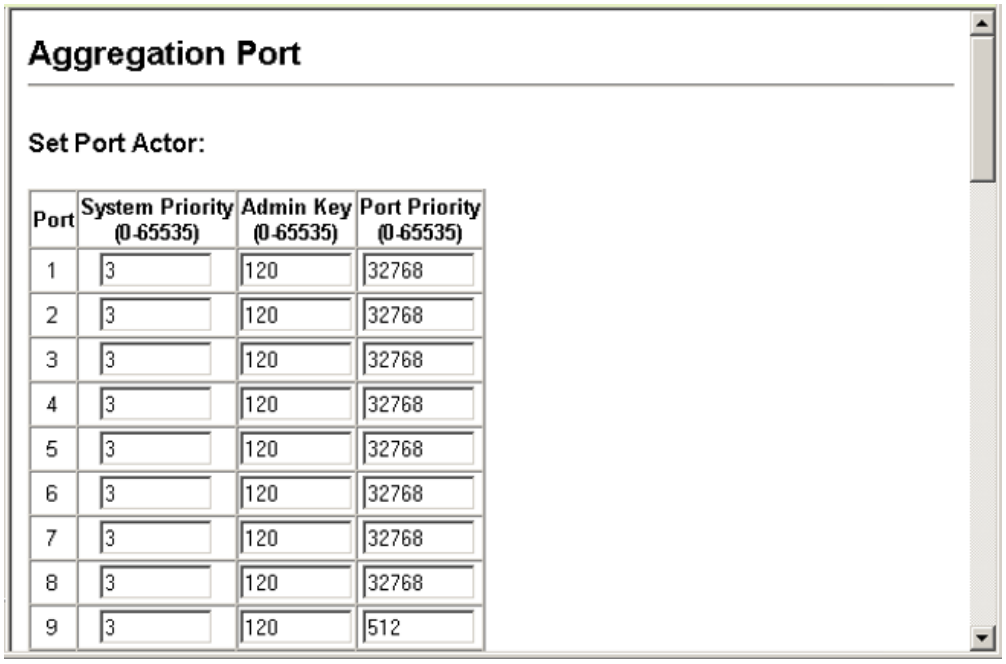
NOTE: Configuring LACP settings for a port only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with that port.

NOTE: Configuring the port partner sets the remote side of an aggregate link; i.e., the ports on the attached device. The command attributes have the same meaning as those used for the port actor.

To configure LACP parameters for group members:

1. Click Port, LACP, Aggregation Port.
2. Set the System Priority, Admin Key, and Port Priority for the Port Actor. You can optionally configure these settings for the Port Partner. (Be aware that these settings only affect the administrative state of the partner, and will not take effect until the next time an aggregate link is formed with this device.)
3. Click Apply.

Figure 115: Configuring LACP Parameters on a Port



CONFIGURING PARAMETERS FOR LACP GROUPS

Use the Port > LACP > Aggregation Group page to set the administrative key for an aggregation group.

CLI REFERENCES

- "lacp admin-key (Port Channel)" on page 707

COMMAND USAGE

Ports are only allowed to join the same Link Aggregation Group (LAG) if (1) the LACP port system priority matches, (2) the LACP port admin key matches, and (3) the LAG admin key matches (if configured). However, if the LAG admin key is set, then the port admin key must be set to the same value for a port to be allowed to join that group.

NOTE: If the LAG admin key is not set when a channel group is formed (i.e., it has a null value of 0), the operational value of this key is set to the same value as the port admin key used by the interfaces that joined the group (see "Configuring Parameters for LACP Group Members").

NOTE: When the LAG is no longer used, the LAG admin key is reset to 0.

PARAMETERS

These parameters are displayed:

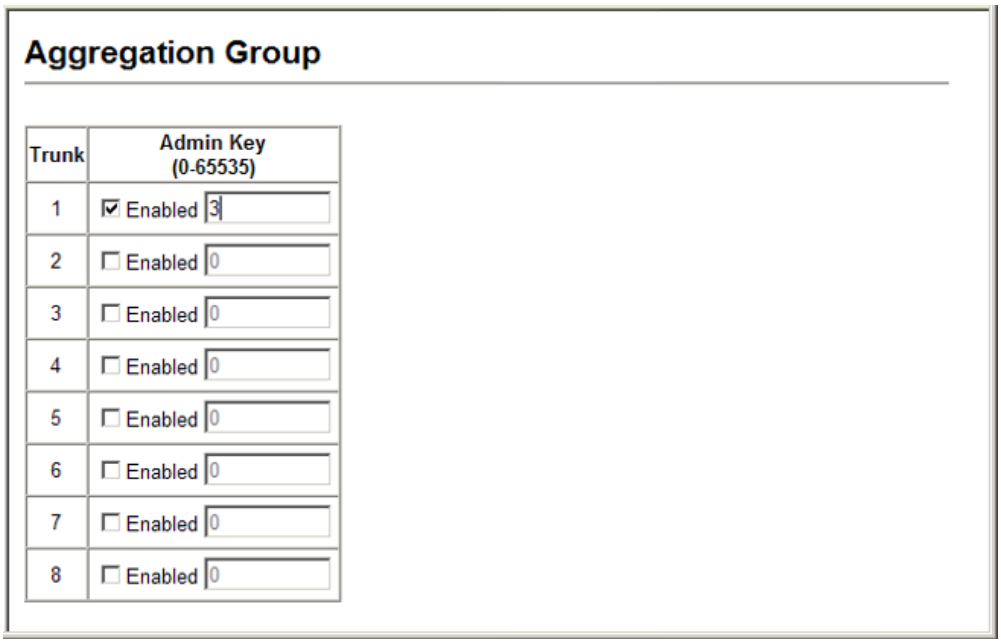
- **Admin Key** – LACP administration key is used to identify a specific link aggregation group (LAG) during local LACP setup on the switch. (Range: 0-65535)

WEB INTERFACE

To configure the admin key for a dynamic trunk:

1. Click Port, LACP, Aggregation Group.
2. Set the Admin Key for the required LACP group.
3. Click Apply.

Figure 116: Configuring the LACP Aggregator Admin Key



DISPLAYING LACP PORT COUNTERS

Use the Port > LACP > Port Counters Information page to display statistics for LACP protocol messages.

CLI REFERENCES

- "show lacp" on page 708

PARAMETERS

These parameters are displayed:

Table 18: LACP Port Counters

Parameter	Description
LACPDUs Sent	Number of valid LACPDUs transmitted from this channel group.
LACPDUs Received	Number of valid LACPDUs received on this channel group.
Marker Sent	Number of valid Marker PDUs transmitted from this channel group.
Marker Received	Number of valid Marker PDUs received by this channel group.

Table 18: LACP Port Counters (Continued)

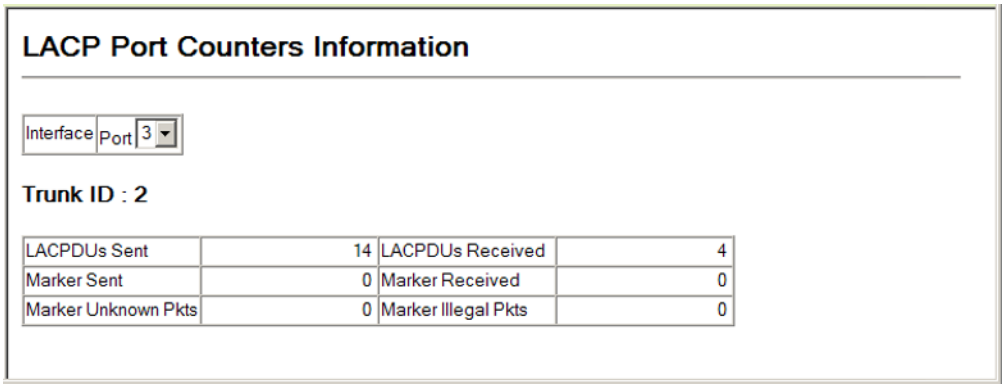
Parameter	Description
Marker Unknown Pkts	Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.
Marker Illegal Pkts	Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.

WEB INTERFACE

To display LACP port counters:

1. Click Port, LACP, Port Counters Information.
2. Select a group member from the Port list.

Figure 117: Displaying LACP Port Counters



DISPLAYING LACP SETTINGS AND STATUS FOR THE LOCAL SIDE

Use the Port > LACP > Port Internal Information page to display the configuration settings and operational state for the local side of a link aggregation.

CLI REFERENCES

- "show lacp" on page 708

PARAMETERS

These parameters are displayed:

Table 19: LACP Internal Configuration Information

Parameter	Description
LACP System Priority	LACP system priority assigned to this port channel.
LACP Port Priority	LACP port priority assigned to this interface within the channel group.
Admin Key	Current administrative value of the key for the aggregation port.
Oper Key	Current operational value of the key for the aggregation port.

Table 19: LACP Internal Configuration Information (Continued)

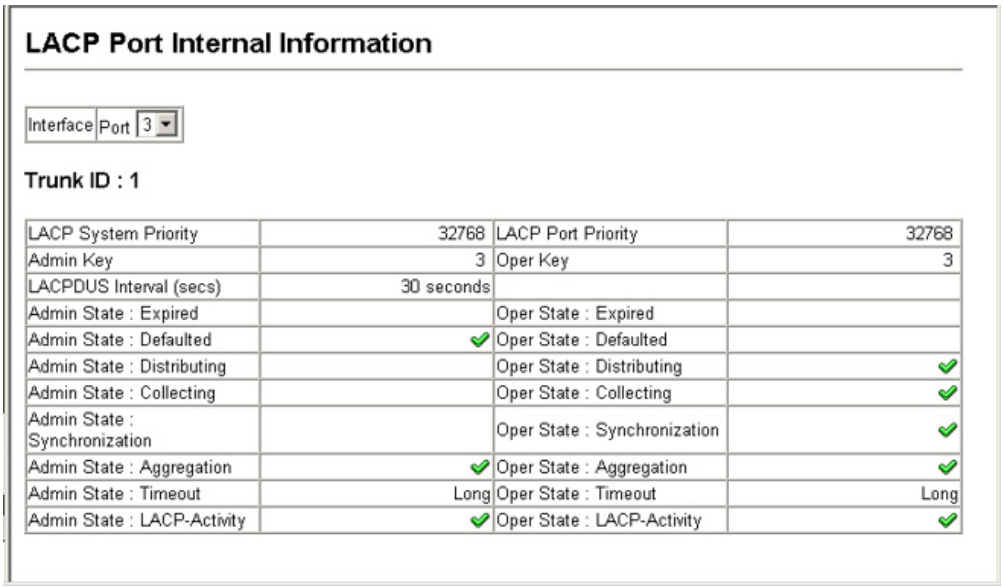
Parameter	Description
LACPDUs Interval	Number of seconds before invalidating received LACPDU information.
Admin State, Oper State	Administrative or operational values of the actor's state parameters: ◆ Expired – The actor's receive machine is in the expired state; ◆ Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner. ◆ Distributing – If false, distribution of outgoing frames on this link is disabled; i.e., distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information. ◆ Collecting – Collection of incoming frames on this link is enabled; i.e., collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. ◆ Synchronization – The System considers this link to be IN_SYNC; i.e., it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted. ◆ Aggregation – The system considers this link to be aggregatable; i.e., a potential candidate for aggregation. ◆ Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate. ◆ LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active)

WEB INTERFACE

To display LACP settings and status for the local side:

1. Click Port, LACP, Port Internal Information.
2. Select a group member from the Port list.

Figure 118: Displaying LACP Port Internal Information



DISPLAYING LACP SETTINGS AND STATUS FOR THE REMOTE SIDE

Use the Port > LACP > Port Neighbors Information page to display the configuration settings and operational state for the remote side of a link aggregation.

CLI REFERENCES

- "show lacp" on page 708

PARAMETERS

These parameters are displayed:

Table 20: LACP Internal Configuration Information

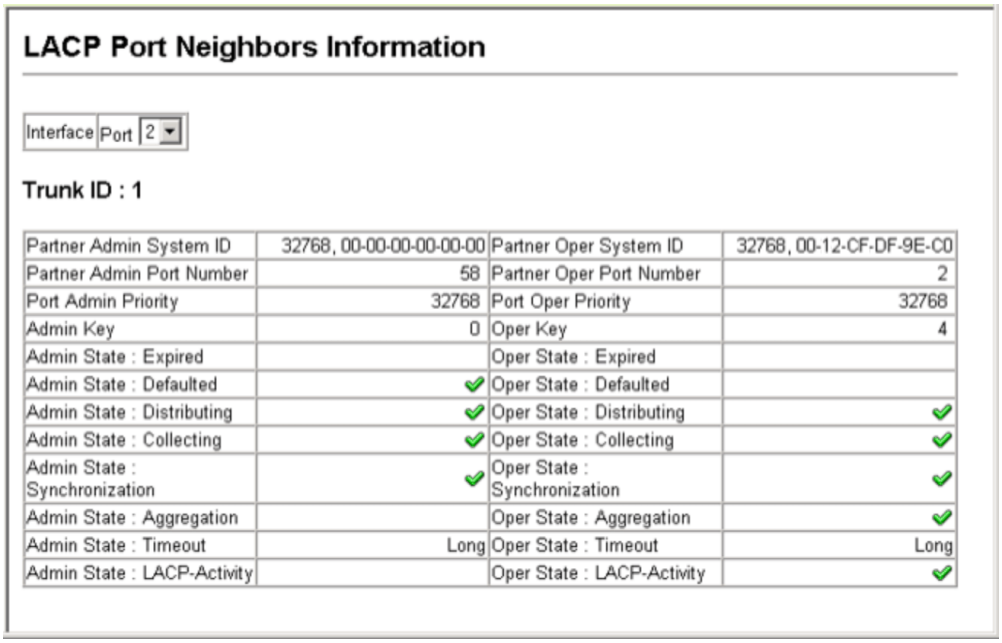
Parameter	Description
Partner Admin System ID	LAG partner's system ID assigned by the user.
Partner Oper System ID	LAG partner's system ID assigned by the LACP protocol.
Partner Admin Port Number	Current administrative value of the port number for the protocol Partner.
Partner Oper Port Number	Operational port number assigned to this aggregation port by the port's protocol partner.
Port Admin Priority	Current administrative value of the port priority for the protocol partner.
Port Oper Priority	Priority value assigned to this aggregation port by the partner.
Admin Key	Current administrative value of the Key for the protocol partner.
Oper Key	Current operational value of the Key for the protocol partner.
Admin State	Administrative values of the partner's state parameters. (See preceding table.)
Oper State	Operational values of the partner's state parameters. (See preceding table.)

WEB INTERFACE

To display LACP settings and status for the remote side:

1. Click Port, LACP, Port Neighbors Information.
2. Select a group member from the Port list.

Figure 119: Displaying LACP Port Remote Information



LACP Port Neighbors Information

Interface Port 2

Trunk ID : 1

Partner Admin System ID	32768, 00-00-00-00-00-00	Partner Oper System ID	32768, 00-12-CF-DF-9E-C0
Partner Admin Port Number	58	Partner Oper Port Number	2
Port Admin Priority	32768	Port Oper Priority	32768
Admin Key	0	Oper Key	4
Admin State : Expired		Oper State : Expired	
Admin State : Defaulted	✓	Oper State : Defaulted	
Admin State : Distributing	✓	Oper State : Distributing	✓
Admin State : Collecting	✓	Oper State : Collecting	✓
Admin State : Synchronization	✓	Oper State : Synchronization	✓
Admin State : Aggregation		Oper State : Aggregation	✓
Admin State : Timeout	Long	Oper State : Timeout	Long
Admin State : LACP-Activity		Oper State : LACP-Activity	✓

STORM CONTROL CONFIGURATION

The switch can be configured to control the maximum amount of traffic caused by broadcast, multicast or unknown unicast storms that will be forwarded.

COMMAND USAGE

Due to an ASIC chip limitation, the supported storm control modes include:

- broadcast
- broadcast + multicast
- broadcast + multicast + unknown unicast

This means that when multicast storm control is enabled, broadcast storm control is also enabled (using the threshold value set by the multicast storm control command). And when unknown unicast storm control is enabled, both broadcast and multicast storm control are also enabled (using the threshold value set by the unknown unicast storm control command).

SETTING BROADCAST STORM THRESHOLDS

Use the Port > Port Broadcast Control or Trunk Broadcast Control page to configure broadcast storm control thresholds. Broadcast storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much broadcast traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from broadcast storms by setting a threshold for broadcast traffic. Any broadcast packets exceeding the specified threshold will then be dropped.

COMMAND USAGE

- Broadcast Storm Control is enabled by default.
- Broadcast control does not effect IP multicast traffic.

CLI REFERENCES

- "switchport packet-rate" on page 690

PARAMETERS

These parameters are displayed:

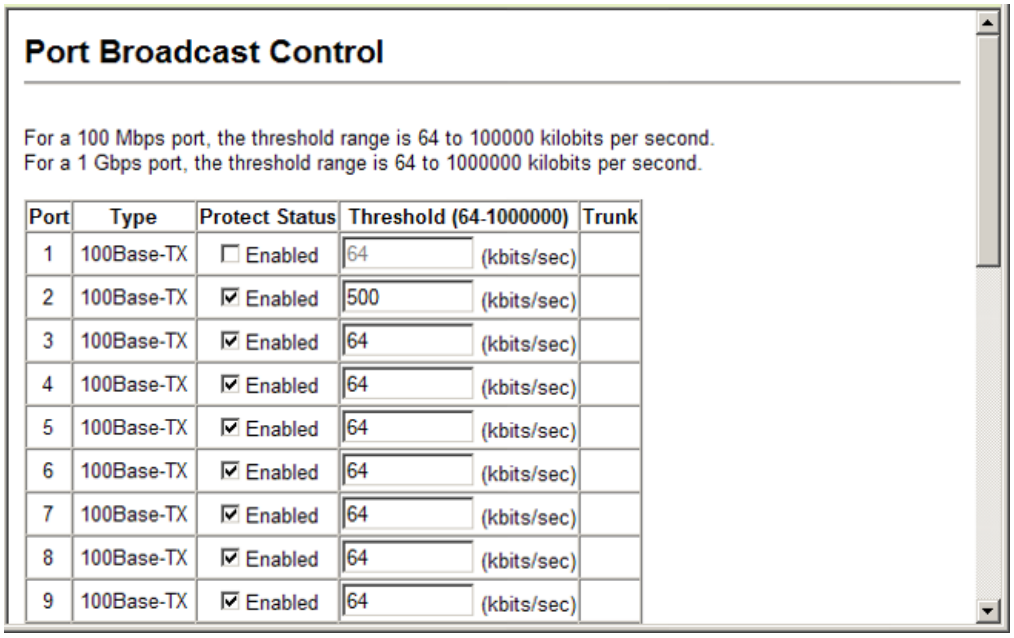
- **Port** – Port number.
- **Type** – Indicates interface type. (100Base-TX, 100Base-T, or SFP)
- **Protect Status** – Enables or disables broadcast storm control. (Default: Enabled)
- **Threshold** – Threshold level as a rate; i.e., kilobits per second. (Range: 64-100000 kilobits per second for Fast Ethernet ports; 64-1000000 kilobits per second for Gigabit ports; Default: 64 kilobits per second)
- **Trunk** – Shows if a port is a trunk member.

WEB INTERFACE

To configure broadcast storm control thresholds:

1. Click Port, Port Broadcast Control.
2. Set the threshold, and mark Enabled for the desired interface.
3. Click Apply.

Figure 120: Configuring Broadcast Storm Control



SETTING MULTICAST STORM THRESHOLDS

Use the Port > Port Multicast Control or Trunk Multicast Control page to protect your network from excess multicast traffic by setting thresholds for each port. Any multicast packets exceeding the specified threshold will then be dropped.

COMMAND USAGE

- Multicast Storm Control is disabled by default.

CLI REFERENCES

- "switchport packet-rate" on page 690

PARAMETERS

These parameters are displayed:

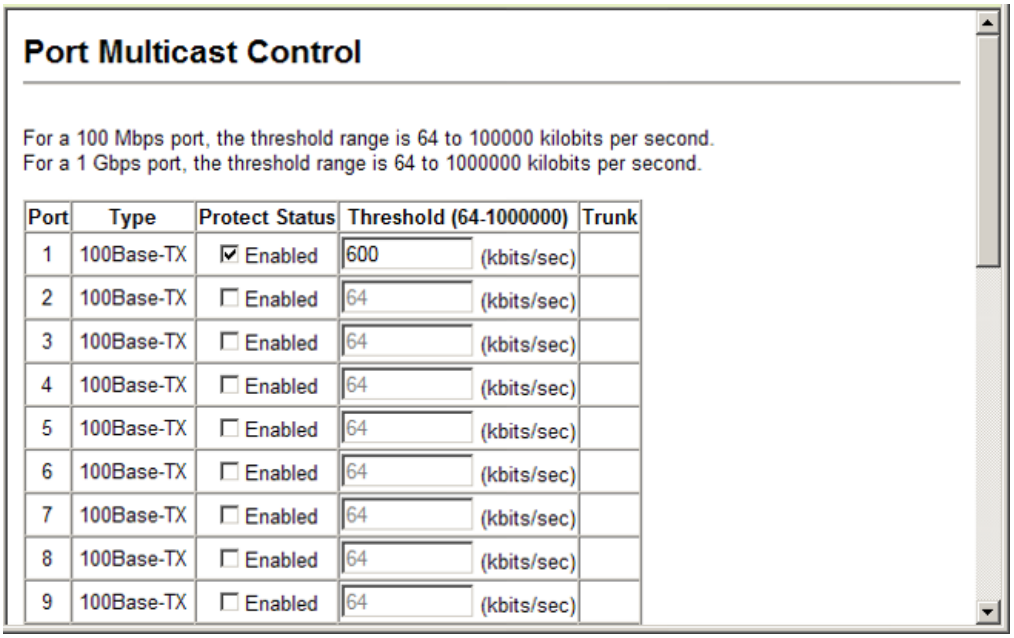
- **Port** – Port number.
- **Type** – Indicates interface type. (100Base-TX, 100Base-T, or SFP)
- **Protect Status** – Enables or disables multicast storm control. (Default: Disabled)
- **Threshold** – Threshold level as a rate; i.e., kilobits per second. (Range: 64-100000 kilobits per second for Fast Ethernet ports; 64-1000000 kilobits per second for Gigabit ports; Default: 64 kilobits per second)
- **Trunk** – Shows if a port is a trunk member.

WEB INTERFACE

To configure multicast storm control thresholds:

1. Click Port, Port Multicast Control.
2. Set the threshold, and mark Enabled for the desired interface.
3. Click Apply.

Figure 121: Configuring Multicast Storm Control



SETTING UNKNOWN UNICAST STORM THRESHOLDS

Use the Port > Port Unknown Unicast Control or Trunk Unknown Unicast Control page to protect your network from excess unknown unicast traffic by setting thresholds for each port. Any unknown unicast packets exceeding the specified threshold will then be dropped.

COMMAND USAGE

- Unknown Unicast Storm Control is disabled by default.

CLI REFERENCES

- "switchport packet-rate" on page 690

PARAMETERS

These parameters are displayed:

- **Port** – Port number.
- **Type** – Indicates interface type. (100Base-TX, 100Base-T, or SFP)
- **Protect Status** – Enables or disables unknown unicast storm control. (Default: Disabled)

- **Threshold** – Threshold level as a rate; i.e., kilobits per second. (Range: 64-100000 kilobits per second for Fast Ethernet ports; 64-1000000 kilobits per second for Gigabit ports; Default: 64 kilobits per second)

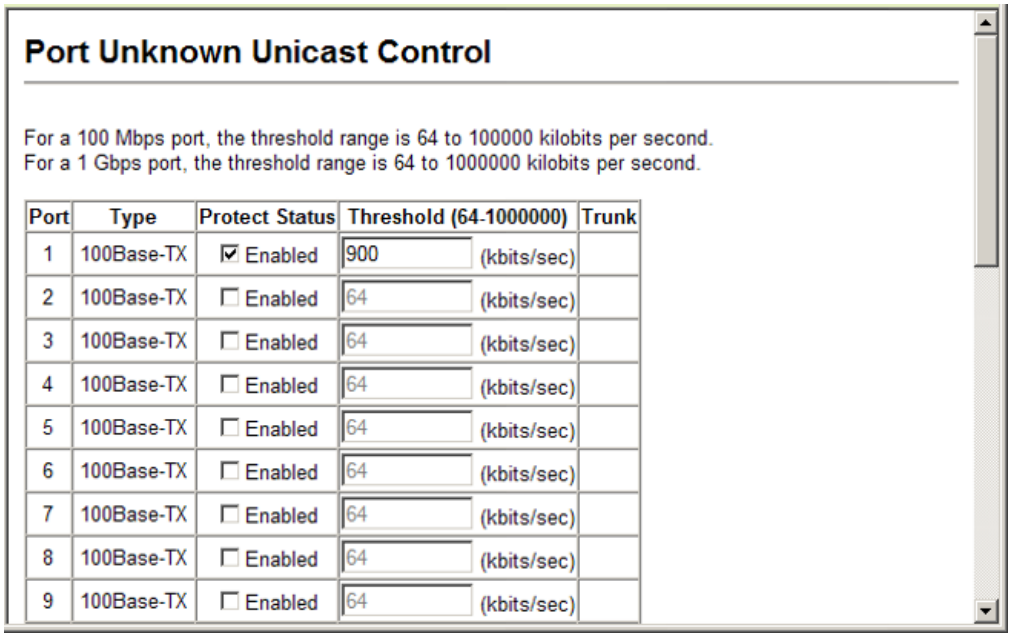
- **Trunk** – Shows if a port is a trunk member.

WEB INTERFACE

To configure unknown unicast storm control thresholds:

1. Click Port, Port Unknown Unicast Control.
2. Set the threshold, and mark Enabled for the desired interface.
3. Click Apply.

Figure 122: Configuring Unknown Unicast Storm Control



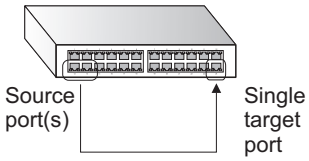
MIRROR CONFIGURATION

The switch can mirror traffic from a source port to a target port, packets containing a specified source address from any port on the switch to a target port, or traffic from one or more source VLANs to a target port. (Port mirroring and MAC address mirroring are described in this section. For information on VLAN mirroring see "Configuring VLAN Mirroring.")

CONFIGURING PORT MIRRORING

Use the Port > Mirror Port Configuration page to mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Figure 123: Configuring Port Mirroring



CLI REFERENCES

- "Port Mirroring Commands" on page 713

COMMAND USAGE

- Traffic can be mirrored from one or more source ports to a destination port on the same switch.
- Monitor port speed should match or exceed source port speed, otherwise traffic may be dropped from the monitor port.
- When mirroring port traffic, the target port must be included in the same VLAN as the source port when using MSTP (see "Spanning Tree Algorithm").
- When mirroring VLAN traffic (see "Configuring VLAN Mirroring") or packets based on a source MAC address (see "Configuring MAC Address Mirroring"), the target port cannot be set to the same target ports as that used for port mirroring by this command.
- When traffic matches the rules for both port mirroring, and for mirroring of VLAN traffic or packets based on a MAC address, the matching packets will not be sent to target port specified for port mirroring.

PARAMETERS

These parameters are displayed:

- **Mirror Sessions** – Displays a list of current mirror sessions.
- **Source Port** – The port whose traffic will be monitored.

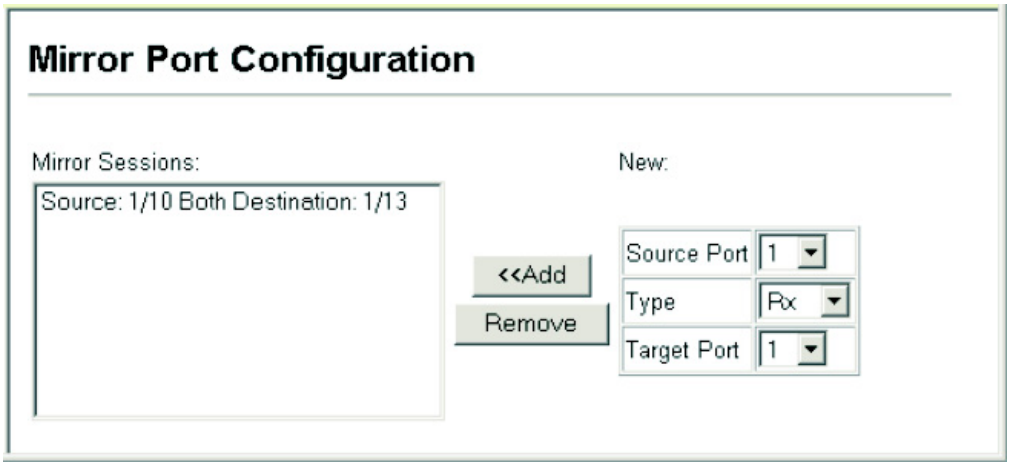
- **Type** – Allows you to select which traffic to mirror to the target port, Rx (receive), Tx (transmit), or Both. (Default: Rx)
- **Target Port** – The port that will mirror the traffic on the source port.

WEB INTERFACE

To configure a mirror session:

1. Click Port, Mirror Port Configuration.
2. Specify the source port.
3. Specify the traffic type to be mirrored.
4. Specify the monitor port.
5. Click Add.

Figure 124: Configuring Port Mirroring



CONFIGURING MAC ADDRESS MIRRORING

Use the Port > MAC Mirror Configuration page to mirror traffic matching a specified source address from any port on the switch to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

CLI REFERENCES

- "Port Mirroring Commands" on page 713

COMMAND USAGE

- When mirroring traffic from a MAC address, ingress traffic with the specified source address entering any port in the switch, other than the target port, will be mirrored to the destination port.
- All mirror sessions must share the same destination port.
- Spanning Tree BPDU packets are not mirrored to the target port.

- When mirroring port traffic, the target port must be included in the same VLAN as the source port when using MSTP (see "Spanning Tree Commands").
- When mirroring VLAN traffic (see "Configuring VLAN Mirroring") or packets based on a source MAC address, the target port cannot be set to the same target ports as that used for port mirroring (see "Configuring Port Mirroring").
- When traffic matches the rules for both port mirroring, and for mirroring of VLAN traffic or packets based on a MAC address, the matching packets will not be sent to target port specified for port mirroring.

PARAMETERS

These parameters are displayed:

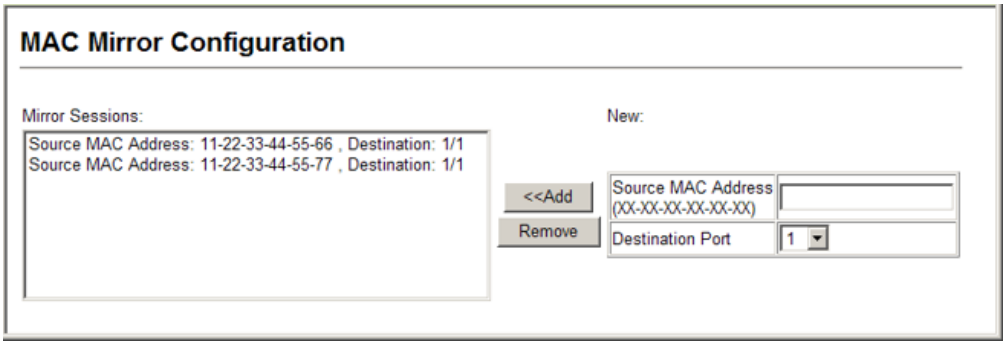
- **Mirror Sessions** – Displays a list of current mirror sessions.
- **Source MAC Address** – MAC address in the form of xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.
- **Destination Port** – The port that will mirror the traffic from the source port. (Range: 1-28/52)

WEB INTERFACE

To mirror packets based on a MAC address:

1. Click Port > MAC Mirror Configuration.
2. Specify the source MAC address and destination port.
3. Click Apply.

Figure 125: Mirroring Packets Based on the Source MAC Address



CONFIGURING RATE LIMITS

Use the Port > Rate Limit pages to apply rate limiting to ingress or egress ports or trunks. This function allows the network manager to control the maximum rate for traffic received or transmitted on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or to trunk groups. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

CLI REFERENCES

- "Rate Limit Commands" on page 717

PARAMETERS

These parameters are displayed:

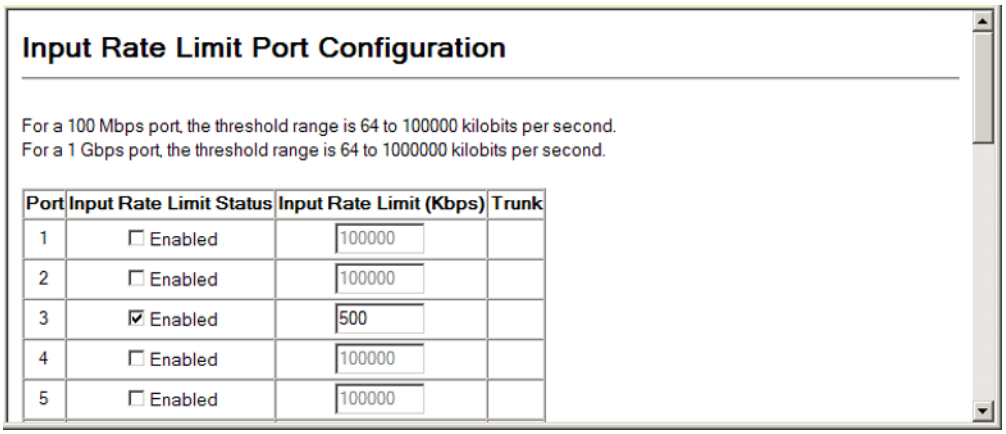
- **Port/Trunk** – Displays the port/trunk number.
- **Rate Limit Status** – Enables or disables the rate limit. (Default: Disabled)
- **Rate Limit** – Sets the rate limit level. (Range: 64 - 100,000 kbits per second for Fast Ethernet ports; 64 - 1,000,000 kbits per second for Gigabit Ethernet ports)

WEB INTERFACE

To configure rate limits:

1. Click Port, Input Port Configuration (or any other rate limit page).
2. Enable the Rate Limit Status for the required ports.
3. set the rate limit for the individual ports.
4. Click Apply.

Figure 126: Configuring Rate Limits



VLAN TRUNKING

Use the Port > Port VLAN Trunking or Trunk VLAN Trunking page to allow unknown VLAN groups to pass through the specified interface.

CLI REFERENCES

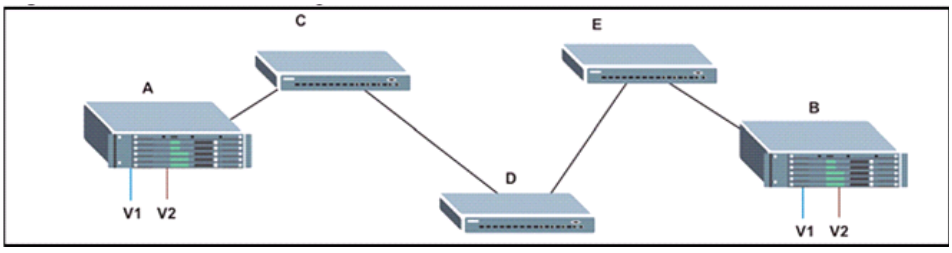
- "vlan-trunking" on page 811

COMMAND USAGE

- Use this feature to configure a tunnel across one or more intermediate switches which pass traffic for VLAN groups to which they do not belong.

  The following figure shows VLANs 1 and 2 configured on switches A and B, with VLAN trunking being used to pass traffic for these VLAN groups across switches C, D and E.

Figure 127: Configuring VLAN Trunking



Without VLAN trunking, you would have to configure VLANs 1 and 2 on all intermediate switches – C, D and E; otherwise these switches would drop any frames with unknown VLAN group tags. However, by enabling VLAN trunking on the intermediate switch ports along the path connecting VLANs 1 and 2, you only need to create these VLAN groups in switches A and B. Switches C, D and E automatically allow frames with VLAN group tags 1 and 2 (groups that are unknown to those switches) to pass through their VLAN trunking ports.

- VLAN trunking is mutually exclusive with the "access" switchport mode (see "Adding Static Members to VLANs"). If VLAN trunking is enabled on an interface, then that interface cannot be set to access mode, and vice versa.
- To prevent loops from forming in the spanning tree, all unknown VLANs will be bound to a single instance (either STP/RSTP or an MSTP instance, depending on the selected STA mode).
- If both VLAN trunking and ingress filtering are disabled on an interface, packets with unknown VLAN tags will still be allowed to enter this interface and will be flooded to all other ports where VLAN trunking is enabled. (In other words, VLAN trunking will still be effectively enabled for the unknown VLAN).

PARAMETERS

These parameters are displayed:

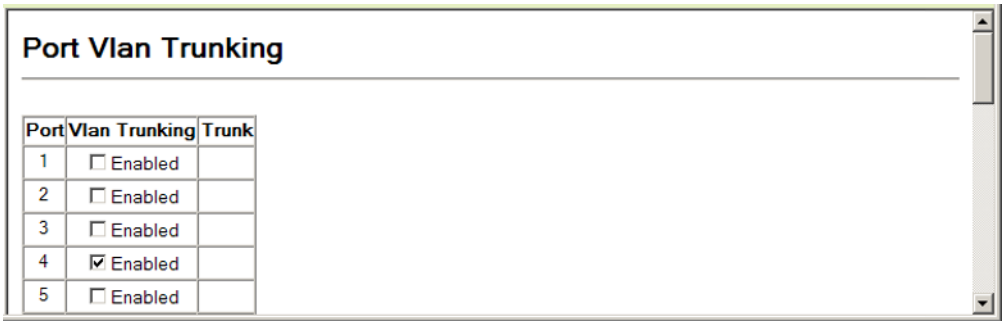
- *Interface* – Port or trunk identifier.
- **VLAN Trunking** – Enables VLAN trunking on the selected interface.

WEB INTERFACE

To enable VLAN trunking on a port or trunk:

1. Click Port, Port VLAN Trunking or Trunk VLAN Trunking.
2. Enable VLAN trunking on any ports or trunk required to establish a path across the switch for unknown VLAN groups.
3. Click Apply.

Figure 128: Configuring VLAN Trunking



PERFORMING CABLE DIAGNOSTICS

Use the Port > Cable Test page to test the cable attached to a port. The cable test will check for any cable faults (short, open, etc.). If a fault is found, the switch reports the length to the fault. It can be used to determine the quality of the cable, connectors, and terminations. Problems such as opens, shorts, and cable impedance mismatch can be diagnosed with this test.

CLI REFERENCES

- "Interface Commands" on page 681

COMMAND USAGE

- Cable diagnostics are performed using Time Domain Reflectometry (TDR) test methods. TDR analyses the cable by sending a pulsed signal into the cable, and then examining the reflection of that pulse.
- This cable test is only accurate for cables 7 - 140 meters long.
- The test takes approximately 5 seconds. The switch displays the results of the test immediately upon completion, including common cable failures, as well as the status and approximate length to a fault.
- Potential conditions which may be listed by the diagnostics include:
  - OK: Correctly terminated pair
  - Open: Open pair, no link partner
  - Short: Shorted pair
  - Open/Short: Open or shorted pair
  - Crosstalk: Abnormal cross-pair coupling
  - Unknown error: Failure condition not determined
  - Test failed: Cable test not supported for this media type.
  - Impedance mismatch: Terminating impedance is not in the reference range.
- Ports are linked down while running cable diagnostics.

PARAMETERS

These parameters are displayed:

- **Port** – Switch port identifier.
- **Type** – Displays media type. (FE – Fast Ethernet, GE – Gigabit Ethernet)

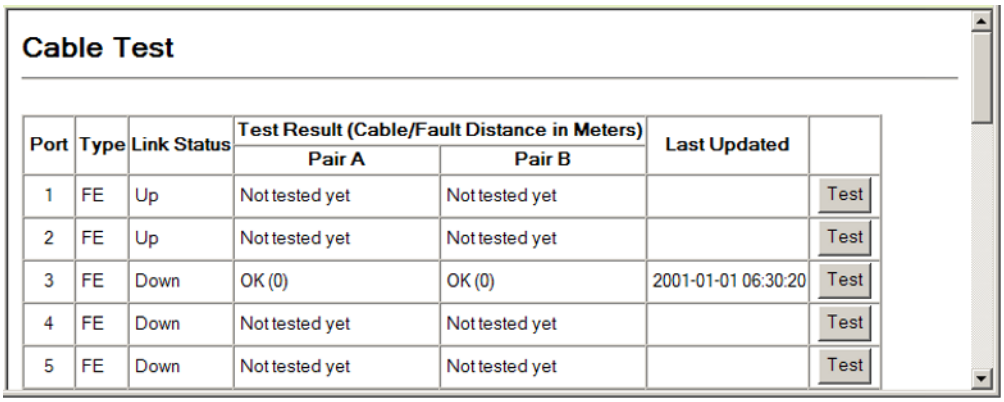
- **Link Status** – Shows if the port link is up or down.
- **Test Result** – The results include common cable failures, as well as the status and approximate distance to a fault, or the approximate cable length if no fault is found.
- **Last Updated** – Shows the last time this port was tested.

WEB INTERFACE

To show a list of port statistics:

1. Click Port, Cable Test.
2. Click Test for any port to start the cable test.

Figure 129: Performing Cable Tests



SHOWING PORT OR TRUNK STATISTICS

Use the Interface > Port/Trunk > Statistics or Chart page to display standard statistics on network traffic from the Interfaces Group and Ethernet-like MIBs, as well as a detailed breakdown of traffic based on the RMON MIB. Interfaces and Ethernet-like statistics display errors on the traffic passing through each port. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port. All values displayed have been accumulated since the last system reboot, and are shown as counts per second. Statistics are refreshed every 60 seconds by default.

NOTE: RMON groups 2, 3 and 9 can only be accessed using SNMP management software.

CLI REFERENCES

- "show interfaces counters" on page 692

PARAMETERS

These parameters are displayed:

Table 21: Port Statistics

Parameter	Description
Interface Statistics	
Received Octets	The total number of octets received on the interface, including framing characters.
Transmitted Octets	The total number of octets transmitted out of the interface, including framing characters.
Received Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Transmitted Errors	The number of outbound packets that could not be transmitted because of errors.
Received Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Transmitted Unicast Packets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Received Discarded Packets	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Transmitted Discarded Packets	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Received Multicast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
Transmitted Multicast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
Received Broadcast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
Transmitted Broadcast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.
Received Unknown Packets	The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.
Etherlike Statistics	
Single Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple Collision Frames	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.

Table 21: Port Statistics (Continued)

Parameter	Description
Frames Too Long	A count of frames received on a particular interface that exceed the maximum permitted frame size.
Alignment Errors	The number of alignment errors (missynchronized data packets).
FCS Errors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
SQE Test Errors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
Internal MAC Receive Errors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error.
Internal MAC Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.
RMON Statistics	
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Received Octets	Total number of octets of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Received Packets	The total number of packets (bad, broadcast and multicast) received.
Broadcast Packets	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Packets	The total number of good packets received that were directed to this multicast address.
Undersize Packets	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Packets	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
64 Bytes Packets	The total number of packets (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Packets 128-255 Byte Packets 256-511 Byte Packets 512-1023 Byte Packets 1024-1518 Byte Packets 1519-1536 Byte Packets	The total number of packets (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).

Table 21: Port Statistics (Continued)

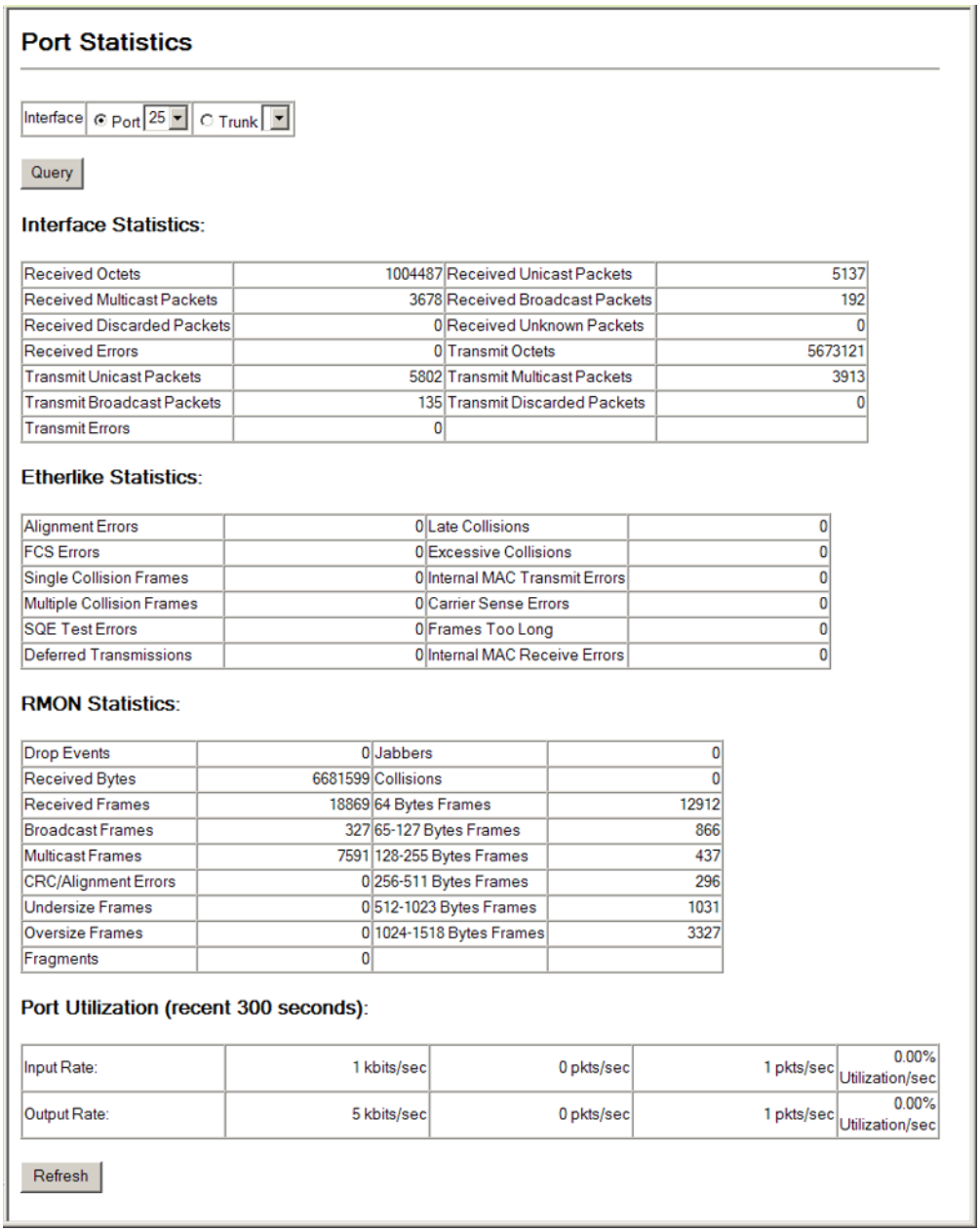
Parameter	Description
Port Utilization	
Input Rate	Shows the ingress rate in kilobits/second, packets/second, and utilization/second.
Output Rate	Shows the egress rate in kilobits/second, packets/second, and utilization/second.

WEB INTERFACE

To show a list of port statistics:

1. Click Port, Port Statistics.
2. Select a port or trunk from the drop-down list.
3. Click Query.
4. Use the Refresh button at the bottom of the page if you need to update the screen.

Figure 130: Showing Port Statistics



Port Statistics

Interface: Port 25 / Trunk

Query

Interface Statistics:

Received Octets	1004487	Received Unicast Packets	5137
Received Multicast Packets	3678	Received Broadcast Packets	192
Received Discarded Packets	0	Received Unknown Packets	0
Received Errors	0	Transmit Octets	5673121
Transmit Unicast Packets	5802	Transmit Multicast Packets	3913
Transmit Broadcast Packets	135	Transmit Discarded Packets	0
Transmit Errors	0		

Etherlike Statistics:

Alignment Errors	0	Late Collisions	0
FCS Errors	0	Excessive Collisions	0
Single Collision Frames	0	Internal MAC Transmit Errors	0
Multiple Collision Frames	0	Carrier Sense Errors	0
SQE Test Errors	0	Frames Too Long	0
Deferred Transmissions	0	Internal MAC Receive Errors	0

RMON Statistics:

Drop Events	0	Jabbers	0
Received Bytes	6681599	Collisions	0
Received Frames	18869	64 Bytes Frames	12912
Broadcast Frames	327	65-127 Bytes Frames	866
Multicast Frames	7591	128-255 Bytes Frames	437
CRC/Alignment Errors	0	256-511 Bytes Frames	296
Undersize Frames	0	512-1023 Bytes Frames	1031
Oversize Frames	0	1024-1518 Bytes Frames	3327
Fragments	0		

Port Utilization (recent 300 seconds):

Input Rate:	1 kbits/sec	0 pkts/sec	1 pkts/sec	0.00% Utilization/sec
Output Rate:	5 kbits/sec	0 pkts/sec	1 pkts/sec	0.00% Utilization/sec

Refresh

9 ADDRESS TABLE SETTINGS

Switches store the addresses for all known devices. This information is used to pass traffic directly between the inbound and outbound ports. All the addresses learned by monitoring traffic are stored in the dynamic address table. You can also manually configure static addresses that are bound to a specific port.

This chapter describes the following topics:

- Static MAC Addresses – Configures static entries in the address table.
- Dynamic Address Cache – Shows dynamic entries in the address table.
- Address Aging Time – Sets timeout for dynamically learned entries.

SETTING STATIC ADDRESSES

Use the Address Table > Static Addresses page to configure static MAC addresses. A static address can be assigned to a specific interface on this switch.

CLI REFERENCES

- "mac-address-table static" on page 740

COMMAND USAGE

The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

- Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.
- Static addresses will not be removed from the address table when a given interface link is down.
- A static address cannot be learned on another port until the address is removed from the table.

PARAMETERS

These parameters are displayed:

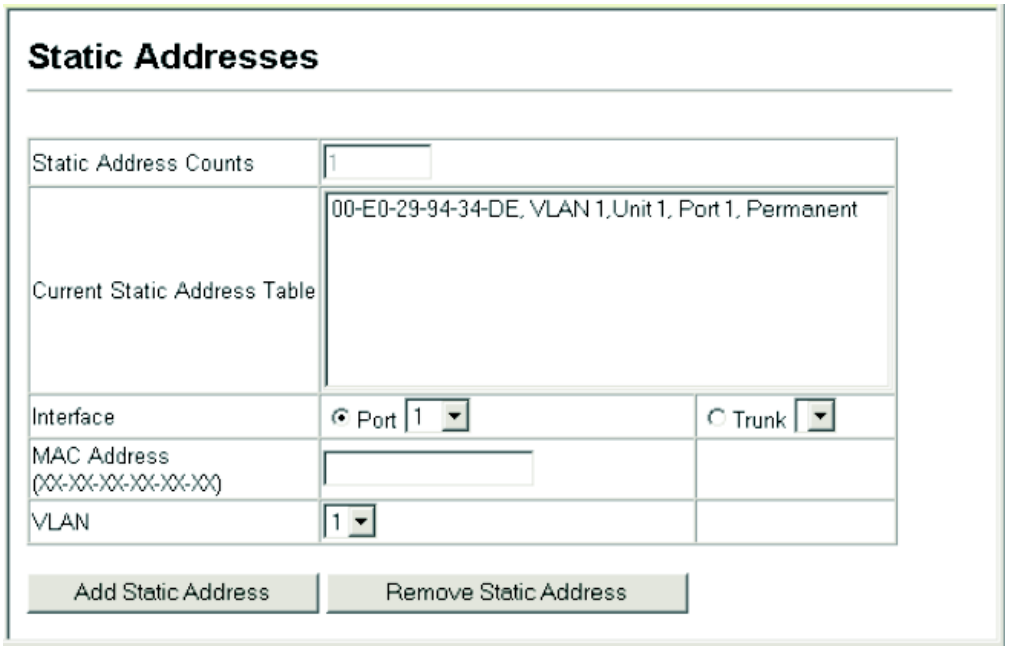
- **Static Address Counts**[7] – The number of manually configured addresses.
- **Current Static Address Table** – Lists all the static addresses.
- **Interface** – Port or trunk associated with the device assigned a static address.
- **MAC Address** – Physical address of a device mapped to this interface. Enter an address in the form of xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.
- **VLAN** – ID of configured VLAN. (Range: 1-4093)

WEB INTERFACE

To configure a static MAC address:

1. Click Address Table, Static Addresses.
2. Select Add from the Action list.
3. Specify the interface, the MAC address and VLAN to which the address will be assigned.
4. Click Add Static Address.

Figure 131: Configuring Static MAC Addresses



7. Web only.

DISPLAYING THE DYNAMIC ADDRESS TABLE

Use the Address Table > Dynamic Addresses page to display the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.

CLI REFERENCES

- "show mac-address-table" on page 741

PARAMETERS

These parameters are displayed:

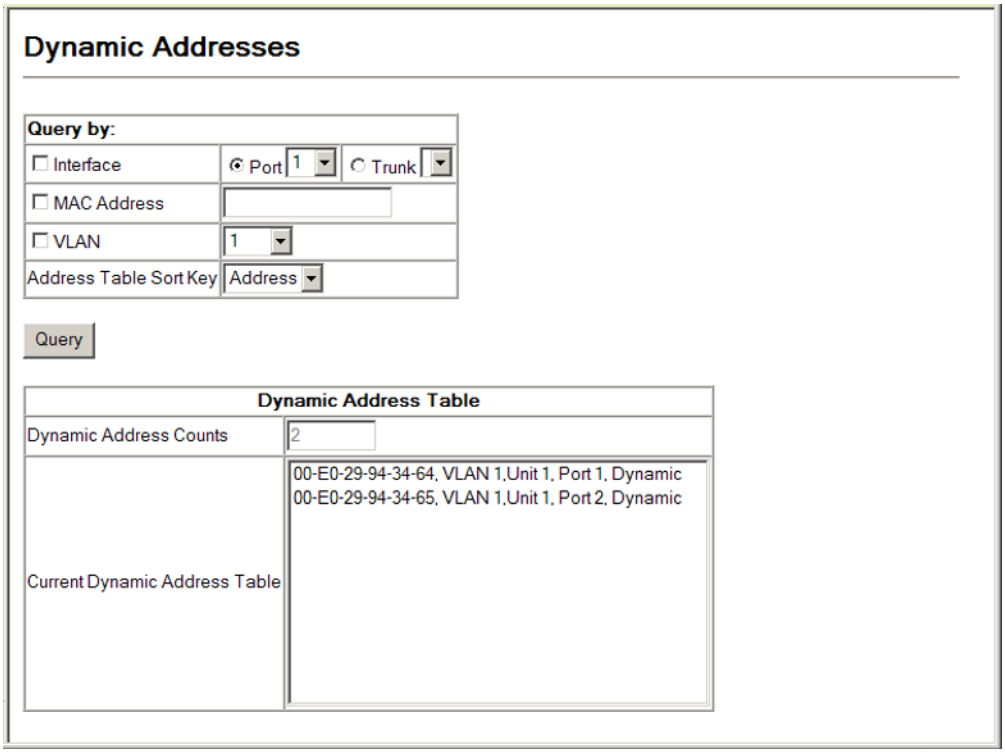
- **Interface** – Indicates a port or trunk.
- **MAC Address** – Physical address associated with this interface.
- **VLAN** – ID of configured VLAN (1-4093).
- **Address Table Sort Key** - You can sort the information displayed based on MAC address, VLAN or interface (port or trunk).
- **Dynamic Address Counts** – The number of addresses dynamically learned.
- **Current Dynamic Address Table** – Lists all the dynamic addresses.

WEB INTERFACE

To show the dynamic address table:

1. Click Address Table, Dynamic Addresses.
2. Select Show Dynamic MAC from the Action list.
3. Specify the search type (i.e., mark the Interface, MAC Address, or VLAN checkbox), select the method of sorting the displayed addresses.
4. Click Query.

Figure 132: Displaying the Dynamic MAC Address Table



CHANGING THE AGING TIME

Use the Address Table > Address Aging page to set the aging time for entries in the dynamic address table. The aging time is used to age out dynamically learned forwarding information.

CLI REFERENCES

- "mac-address-table aging-time" on page 739

PARAMETERS

These parameters are displayed:

- **Aging Status** – Enables/disables the aging function.
- **Aging Time** – The time after which a learned entry is discarded. (Range: 10-844 seconds; Default: 300 seconds)

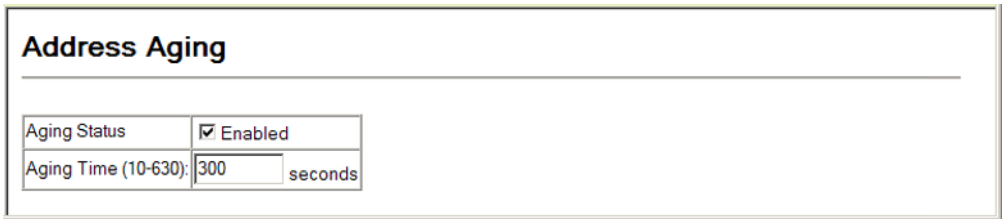
WEB INTERFACE

To set the aging time for entries in the dynamic address table:

1. Click Address Table, Address Aging.
2. Modify the aging status if required.
3. Specify a new aging time.

4. Click Apply.

Figure 133: Setting the Address Aging Time



10 SPANNING TREE ALGORITHM

This chapter describes the following basic topics:

- Loopback Detection – Configures detection and response to loopback BPDUs.
- Global Settings for STA – Configures global bridge settings for STP, RSTP and MSTP.
- Interface Settings for STA – Configures interface settings for STA, including priority, path cost, link type, and designation as an edge port.
- Global Settings for MSTP – Sets the VLANs and associated priority assigned to an MST instance
- Interface Settings for MSTP – Configures interface settings for MSTP, including priority and path cost.

OVERVIEW

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

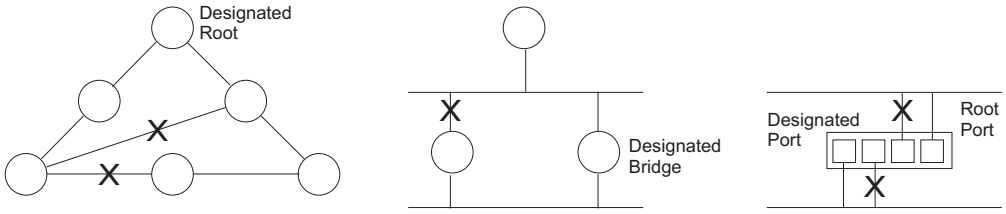
The spanning tree algorithms supported by this switch include these versions:

- STP – Spanning Tree Protocol (IEEE 802.1D)
- RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)
- MSTP – Multiple Spanning Tree Protocol (IEEE 802.1s)

STP – STP uses a distributed algorithm to select a bridging device (STP-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the

lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

Figure 134: STP Root Ports and Designated Ports

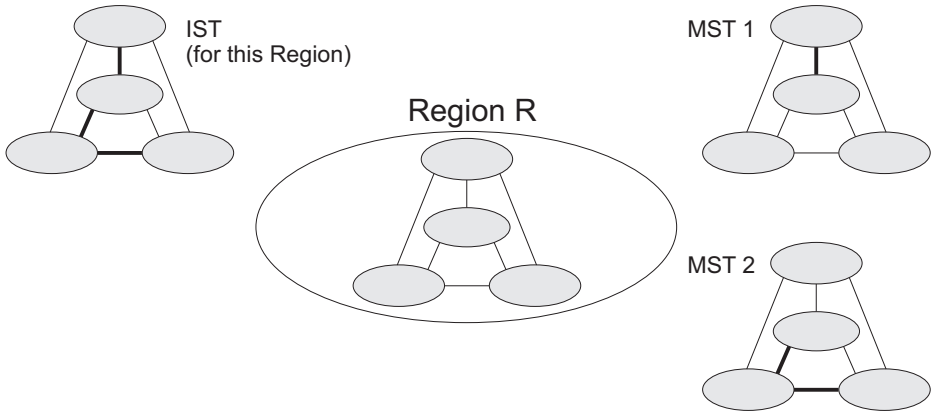


Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

RSTP – RSTP is designed as a general replacement for the slower, legacy STP. RSTP is also incorporated into MSTP. RSTP achieves much faster reconfiguration (i.e., around 1 to 3 seconds, compared to 30 seconds or more for STP) by reducing the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails, and retaining the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

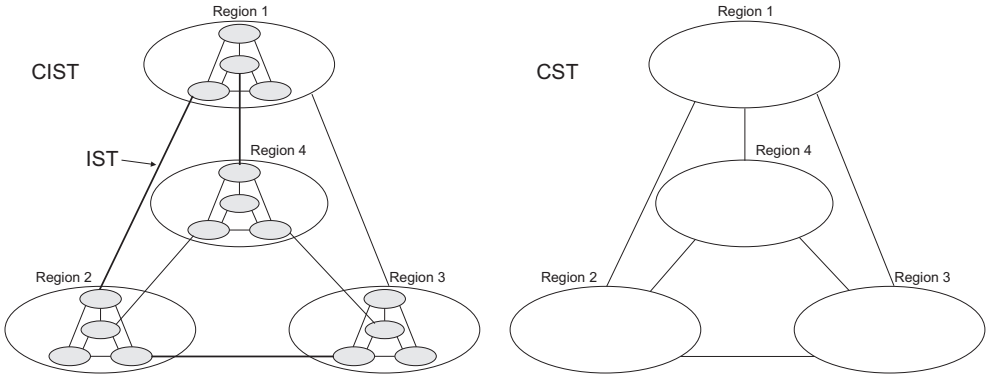
MSTP – When using STP or RSTP, it may be difficult to maintain a stable path between all VLAN members. Frequent changes in the tree structure can easily isolate some of the group members. MSTP (which is based on RSTP for fast convergence) is designed to support independent spanning trees based on VLAN groups. Using multiple spanning trees can provide multiple forwarding paths and enable load balancing. One or more VLANs can be grouped into a Multiple Spanning Tree Instance (MSTI). MSTP builds a separate Multiple Spanning Tree (MST) for each instance to maintain connectivity among each of the assigned VLAN groups. MSTP then builds a Internal Spanning Tree (IST) for the Region containing all commonly configured MSTP bridges.

Figure 135: MSTP Region, Internal Spanning Tree, Multiple Spanning Tree



An MST Region consists of a group of interconnected bridges that have the same MST Configuration Identifiers (including the Region Name, Revision Level and Configuration Digest – see "Configuring Multiple Spanning Trees"). An MST Region may contain multiple MSTP Instances. An Internal Spanning Tree (IST) is used to connect all the MSTP switches within an MST region. A Common Spanning Tree (CST) interconnects all adjacent MST Regions, and acts as a virtual bridge node for communications with STP or RSTP nodes in the global network.

Figure 136: Common Internal Spanning Tree, Common Spanning Tree, Internal Spanning Tree



MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree (CIST). The CIST is formed as a result of the running spanning tree algorithm between switches that support the STP, RSTP, MSTP protocols.

Once you specify the VLANs to include in a Multiple Spanning Tree Instance (MSTI), the protocol will automatically build an MSTI tree to maintain connectivity among each of the VLANs. MSTP maintains contact with the global network because each instance is treated as an RSTP node in the Common Spanning Tree (CST).

CONFIGURING LOOPBACK DETECTION

Use the Spanning Tree > Port Loopback Detection or Trunk Loopback Detection page to configure loopback detection on an interface. When loopback detection is enabled and a port or trunk receives it's own BPDU, the detection agent drops the loopback BPDU, sends an SNMP trap, and places the interface in discarding mode. This loopback state can be released manually or automatically. If the interface is configured for automatic loopback release, then the port will only be returned to the forwarding state if one of the following conditions is satisfied:

- The interface receives any other BPDU except for it's own, or;
- The interfaces's link status changes to link down and then link up again, or;
- The interface ceases to receive it's own BPDUs in a forward delay interval.

NOTE: If loopback detection is not enabled and an interface receives it's own BPDU, then the interface will drop the loopback BPDU according to IEEE Standard 802.1w-2001 9.3.4 (Note 1).

NOTE: Loopback detection will not be active if Spanning Tree is disabled on the switch.

NOTE: When configured for manual release mode, then a link down/up event will not release the port from the discarding state.

CLI REFERENCES

- "Spanning Tree Commands" on page 743

PARAMETERS

These parameters are displayed:

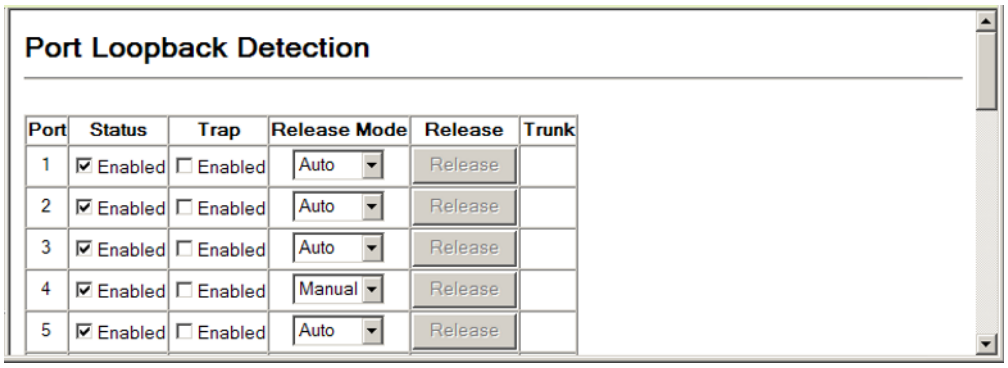
- **Port/Trunk** – Displays a list of ports or trunks.
- **Status** – Enables loopback detection on this interface. (Default: Enabled)
- **Trap** – Enables SNMP trap notification for loopback events on this interface. (Default: Disabled)
- **Release Mode** – Configures the interface for automatic or manual loopback release. (Default: Auto)
- **Release** – Allows an interface to be manually released from discard mode. This is only available if the interface is configured for manual release mode.

WEB INTERFACE

To configure loopback detection:

1. Click Spanning Tree, Port Loopback Detection.
2. Modify the required loopback detection attributes.
3. Click Apply

Figure 137: Configuring Port Loopback Detection



DISPLAYING GLOBAL SETTINGS FOR STA

Use the Spanning Tree > STA > Information page to display a summary of the current bridge STA information that applies to the entire switch.

CLI REFERENCES

- "show spanning-tree" on page 768
- "show spanning-tree mst configuration" on page 770

PARAMETERS

The parameters displayed are described in the preceding section, except for the following items:

- **Spanning Tree State** – Shows if the switch is enabled to participate in an STA-compliant network.
- **Bridge ID** – A unique identifier for this bridge, consisting of the bridge priority, the MST Instance ID 0 for the Common Spanning Tree when spanning tree type is set to MSTP, and MAC address (where the address is taken from the switch system).
- **Max Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to

"ports" in this section mean "interfaces," which includes both ports and trunks.)

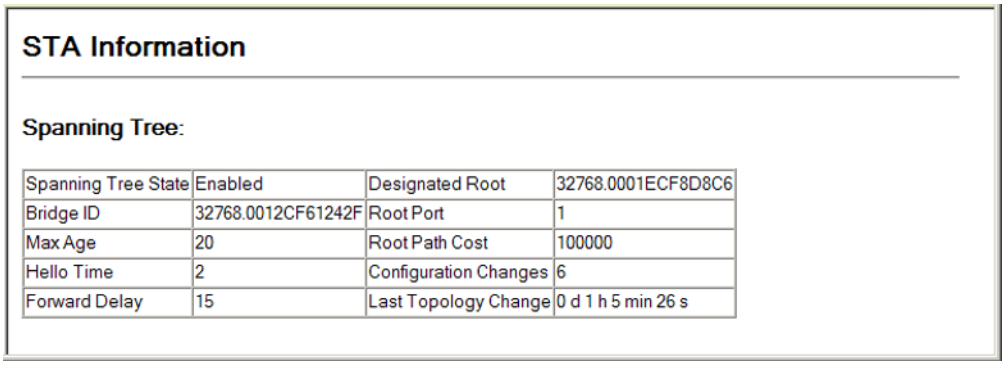
- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.
- **Forward Delay** – The maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
- **Designated Root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
- **Root Port** – The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.
- **Root Path Cost** – The path cost from the root port on this switch to the root device.
- **Configuration Changes** – The number of times the Spanning Tree has been reconfigured.
- **Last Topology Change** – Time since the Spanning Tree was last reconfigured.

WEB INTERFACE

To display global STA settings:

1. Click Spanning Tree, STA, Information.

Figure 138: Displaying Global Settings for STA



CONFIGURING GLOBAL SETTINGS FOR STA

Use the Spanning Tree > STA > Configuration page to configure global settings for the spanning tree that apply to the entire switch.

CLI REFERENCES

- "Spanning Tree Commands" on page 743

COMMAND USAGE

- Spanning Tree Protocol[8]

  Uses RSTP for the internal state machine, but sends only 802.1D BPDUs. This creates one spanning tree instance for the entire network. If multiple VLANs are implemented on a network, the path between specific VLAN members may be inadvertently disabled to prevent network loops, thus isolating group members. When operating multiple VLANs, we recommend selecting the MSTP option.

- Rapid Spanning Tree Protocol[8]

  RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:

  - STP Mode – If the switch receives an 802.1D BPDU (i.e., STP BPDU) after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.

  - RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

- Multiple Spanning Tree Protocol

  MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.

  - To allow multiple spanning trees to operate over the network, you must configure a related set of bridges with the same MSTP configuration, allowing them to participate in a specific set of spanning tree instances.

  - A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments.

8. STP and RSTP BPDUs are transmitted as untagged frames, and will cross any VLAN boundaries.

- Be careful when switching between spanning tree modes. Changing modes stops all spanning-tree instances for the previous mode and restarts the system in the new mode, temporarily disrupting user traffic.

PARAMETERS

These parameters are displayed:

Basic Settings

- **Spanning Tree Status** – Enables/disables STA on this switch. (Default: Enabled)
- **Spanning Tree Type** – Specifies the type of spanning tree used on this switch:
  - **STP**: Spanning Tree Protocol (IEEE 802.1D); i.e., when this option is selected, the switch will use RSTP set to STP forced compatibility mode).
  - **RSTP**: Rapid Spanning Tree (IEEE 802.1w); RSTP is the default.
  - **MSTP**: Multiple Spanning Tree (IEEE 802.1s)
- **Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. (Note that lower numeric values indicate higher priority.)
  - Default: 32768
  - Range: 0-61440, in steps of 4096
  - Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440
- **Spanning Tree BPDU Flooding** – Configures the system to flood BPDUs to all other ports on the switch or just to all other ports in the same VLAN when spanning tree is disabled globally on the switch or disabled on a specific port.
  - To VLAN: Floods BPDUs to all other ports within the receiving port's native VLAN (i.e., as determined by port's PVID). This is the default.
  - To All: Floods BPDUs to all other ports on the switch.

  The setting has no effect if BPDU flooding is disabled on a port (see "Configuring Interface Settings for STA").

When the Switch Becomes Root

- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.
  - Default: 2
  - Minimum: 1
  - Maximum: The lower of 10 or [(Max. Message Age / 2) -1]

- **Maximum Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to "ports" in this section mean "interfaces," which includes both ports and trunks.)
  - Default: 20
  - Minimum: The higher of 6 or [2 x (Hello Time + 1)]
  - Maximum: The lower of 40 or [2 x (Forward Delay - 1)]

- **Forward Delay** – The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
  - Default: 15
  - Minimum: The higher of 4 or [(Max. Message Age / 2) + 1]
  - Maximum: 30

RSTP Configuration

NOTE: The following commands also apply to MSTP which is based upon RSTP, and STP which is a backwards-compatible subset of RSTP.

- **Path Cost Method** – The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.
  - Long: Specifies 32-bit based values that range from 1-200,000,000. (This is the default.)
  - Short: Specifies 16-bit based values that range from 1-65535.

- **Transmission Limit** – The maximum transmission rate for BPDUs is specified by setting the minimum interval between the transmission of consecutive protocol messages. (Range: 1-10; Default: 3)

Configuration Settings for MSTP

- **Max Instance Numbers** – The maximum number of MSTP instances to which this switch can be assigned.

- **Configuration Digest** – An MD5 signature key that contains the VLAN ID to MST ID mapping table. In other words, this key is a mapping of all VLANs to the CIST.

- **Region Revision**[9] – The revision for this MSTI. (Range: 0-65535; Default: 0)
- **Region Name**[9] – The name for this MSTI. (Maximum length: 32 characters; switch's MAC address)
- **Maximum Hop Count** – The maximum number of hops allowed in the MST region before a BPDU is discarded. (Range: 1-40; Default: 20)

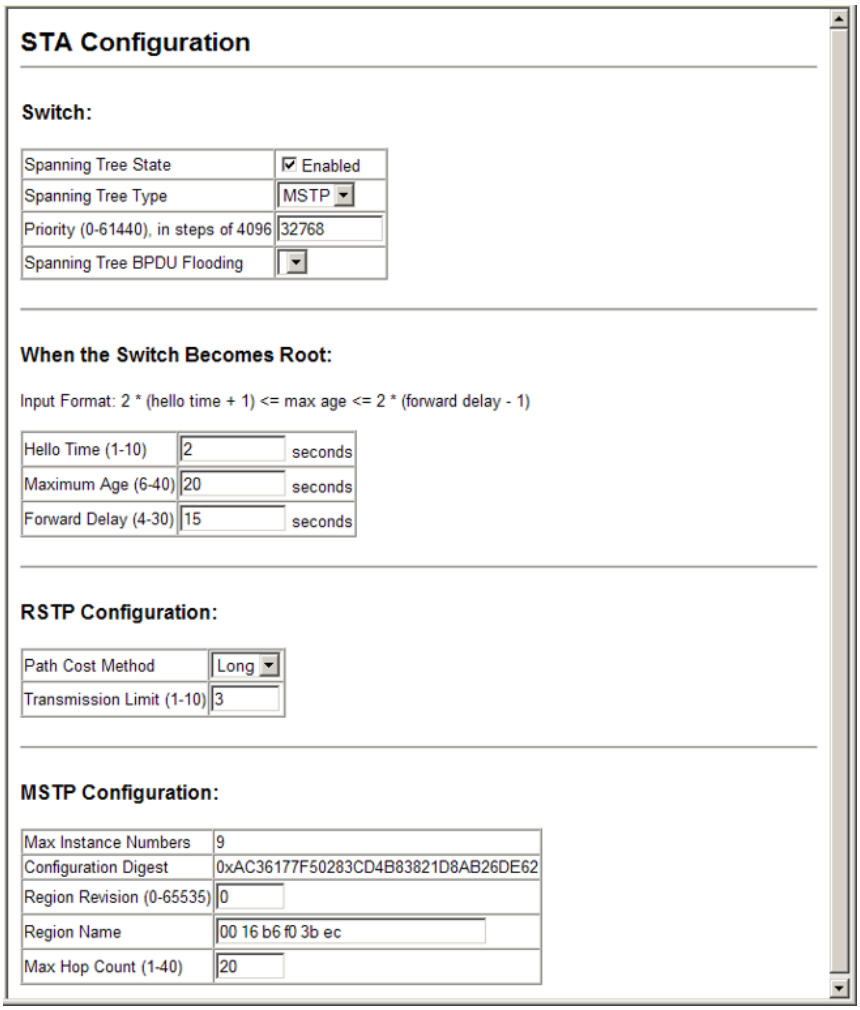
WEB INTERFACE

To configure global STA settings:

1. Click Spanning Tree, STA.
2. Select Configure Global from the Step list.
3. Select Configure from the Action list.
4. Modify any of the required attributes. Note that the parameters displayed for the spanning tree types (STP, RSTP, MSTP) varies as described in the preceding section.
5. Click Apply

9. The MST name and revision number are both required to uniquely identify an MST region.

Figure 139: Configuring Global Settings for STA



DISPLAYING INTERFACE SETTINGS FOR STA

Use the Spanning Tree > STA > Port Information page to display the current status of ports or trunks in the Spanning Tree.

CLI REFERENCES

- "show spanning-tree" on page 768

PARAMETERS

These parameters are displayed:

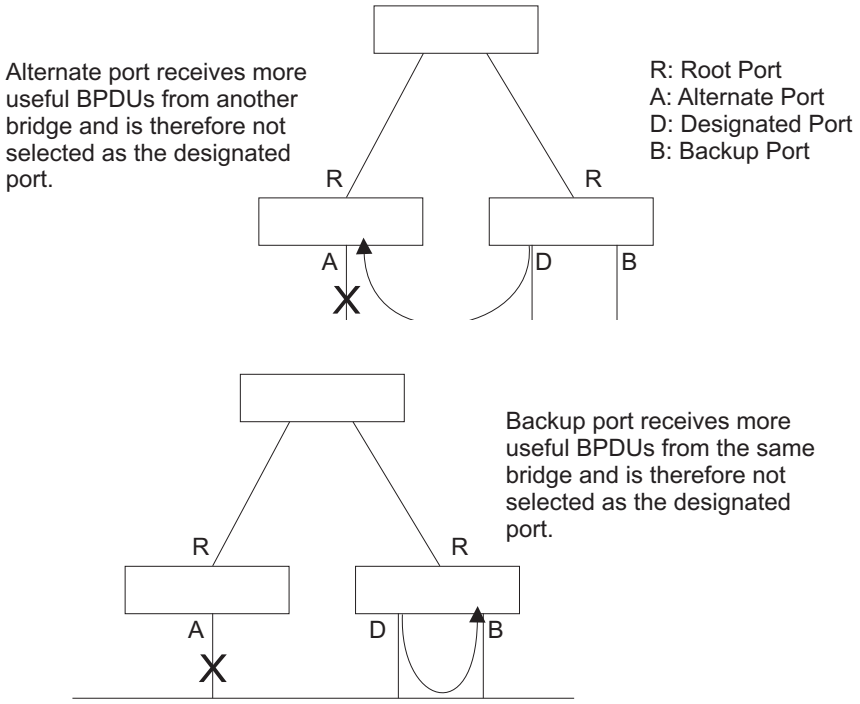
- **Spanning Tree** – Shows if STA has been enabled on this interface.
- **BPDU Flooding** – Shows if BPDUs will be flooded to other ports when spanning tree is disabled globally on the switch or disabled on a specific port.

- **STA Status** – Displays current state of this port within the Spanning Tree:
  - **Discarding** - Port receives STA configuration messages, but does not forward packets.
  - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** - Port forwards packets, and continues learning addresses.

  The rules defining port status are:
  - A port on a network segment with no other STA compliant bridging device is always forwarding.
  - If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is discarding.
  - All ports are discarding when the switch is booted, then some of them change state to learning, and then to forwarding.
- **Forward Transitions** – The number of times this port has transitioned from the Learning state to the Forwarding state.
- **Designated Cost** – The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
- **Designated Bridge** – The bridge priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.
- **Designated Port** – The port priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.
- **Oper Path Cost** – The contribution of this port to the path cost of paths towards the spanning tree root which include this port.
- **Oper Link Type** – The operational point-to-point status of the LAN segment attached to this interface. This parameter is determined by manual configuration or by auto-detection, as described for Admin Link Type in STA Port Configuration on page 312.
- **Oper Edge Port** – This parameter is initialized to the setting for Admin Edge Port in STA Port Configuration on page 312 (i.e., true or false), but will be set to false if a BPDU is received, indicating that another bridge is attached to this port.

- **Port Role** – Roles are assigned according to whether the port is part of the active topology connecting the bridge to the root bridge (i.e., **root** port), connecting a LAN through the bridge to the root bridge (i.e., **designated** port), is the MSTI regional root (i.e., **master** port), or is an **alternate** or **backup** port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed. The role is set to disabled (i.e., **disabled** port) if a port has no role within the spanning tree.

Figure 140: STA Port Roles



WEB INTERFACE

To display interface settings for STA:

1. Click Spanning Tree, STA, Port Information.

Figure 141: Displaying Interface Settings for STA

STA Port Information

Port	Spanning Tree	BPDU Flooding	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Enabled	Enabled	Forwarding	1	0	32768.0001ECF8D8C6	128.14	100000	Point-to-Point	Disabled	Root	
2	Enabled	Enabled	Forwarding	1	100000	32768.0012CF61242F	128.2	100000	Point-to-Point	Enabled	Designated	
3	Enabled	Enabled	Forwarding	6	100000	32768.0012CF61242F	128.3	100000	Point-to-Point	Disabled	Designated	
4	Enabled	Enabled	Discarding	0	100000	32768.0012CF61242F	128.4	100000	Point-to-Point	Enabled	Disabled	
5	Enabled	Enabled	Discarding	0	100000	32768.0012CF61242F	128.5	100000	Point-to-Point	Enabled	Disabled	
6	Enabled	Enabled	Discarding	0	100000	32768.0012CF61242F	128.6	100000	Point-to-Point	Enabled	Disabled	
7	Enabled	Enabled	Discarding	0	100000	32768.0012CF61242F	128.7	100000	Point-to-Point	Enabled	Disabled	
8	Enabled	Enabled	Discarding	0	100000	32768.0012CF61242F	128.8	100000	Point-to-Point	Enabled	Disabled	
9	Enabled	Enabled	Discarding	0	100000	32768.0012CF61242F	128.9	100000	Point-to-Point	Enabled	Disabled	
10	Enabled	Enabled	Discarding	0	100000	32768.0012CF61242F	128.10	100000	Point-to-Point	Enabled	Disabled	

CONFIGURING INTERFACE SETTINGS FOR STA

Use the Spanning Tree > STA > Port Configuration page to configure STA attributes for specific interfaces, including port priority, path cost, link type, and edge port. You may use a different priority or path cost for ports of the same media type to indicate the preferred path, link type to indicate a point-to-point connection or shared-media connection, and edge port to indicate if the attached device can support fast forwarding. (References to "ports" in this section means "interfaces," which includes both ports and trunks.)

CLI REFERENCES

- "Spanning Tree Commands" on page 743

PARAMETERS

These parameters are displayed:

- *Interface* – Displays a list of ports or trunks.
- **Spanning Tree** – Enables/disables STA on this interface. (Default: Enabled)
- **BPDU Flooding** - Enables/disables the flooding of BPDUs to other ports when global spanning tree is disabled (page 305) or when spanning tree is disabled on specific port. When flooding is enabled, BPDUs are flooded to all other ports on the switch or to all other ports within the receiving port's native VLAN as specified by the Spanning Tree BPDU Flooding attribute (page 305).
- **STA State** – Displays current state of this port within the Spanning Tree. (See "Displaying Interface Settings for STA" for additional information.)
  - **Discarding** - Port receives STA configuration messages, but does not forward packets.
  - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** - Port forwards packets, and continues learning addresses.
- **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.
  - Default: 128
  - Range: 0-240, in steps of 16

- **Admin Path Cost** – This parameter is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Note that path cost takes precedence over port priority. (Range: 0 for auto-configuration, 1-65535 for the short path cost method[10], 1-200,000,000 for the long path cost method)

  By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

Table 22: Recommended STA Path Cost Range

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

Table 23: Recommended STA Path Costs

Port Type	Link Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex	100	2,000,000
	Full Duplex	95	1,999,999
	Trunk	90	1,000,000
Fast Ethernet	Half Duplex	19	200,000
	Full Duplex	18	100,000
	Trunk	15	50,000
Gigabit Ethernet	Full Duplex	4	10,000
	Trunk	3	5,000

Table 24: Default STA Path Costs

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex	2,000,000
	Full Duplex	1,000,000
	Trunk	500,000
Fast Ethernet	Half Duplex	200,000
	Full Duplex	100,000
	Trunk	50,000
Gigabit Ethernet	Full Duplex	10,000
	Trunk	5,000

10. Refer to "Configuring Global Settings for STA" for information on setting the path cost method.

- **Admin Link Type** – The link type attached to this interface.
  - Point-to-Point – A connection to exactly one other bridge.
  - Shared – A connection to two or more bridges.
  - Auto – The switch automatically determines if the interface is attached to a point-to-point link or to shared media. (This is the default setting.)

- **Root Guard** – STA allows a bridge with a lower bridge identifier (or same identifier and lower MAC address) to take over as the root bridge at any time. Root Guard can be used to ensure that the root bridge is not formed at a suboptimal location. Root Guard should be enabled on any designated port connected to low-speed bridges which could potentially overload a slower link by taking over as the root port and forming a new spanning tree topology. It could also be used to form a border around part of the network where the root bridge is allowed. (Default: Disabled)

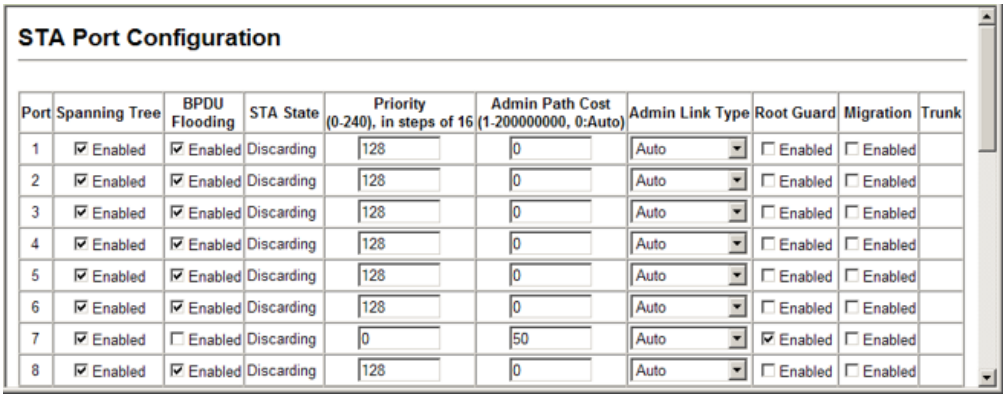
- **Migration** – If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the Protocol Migration button to manually re-check the appropriate BPDU format (RSTP or STP-compatible) to send on the selected interfaces. (Default: Disabled)

WEB INTERFACE

To configure interface settings for STA:

1. Click Spanning Tree, STA, Port Configuration or Trunk Configuration.
2. Modify any of the required attributes.
3. Click Apply.

Figure 142: Configuring Interface Settings for STA



SPANNING TREE EDGE PORT CONFIGURATION

Use the Spanning Tree > STA > Port Edge Port Configuration or Trunk Edge Port Configuration page to enable additional STA options when an interface is attached to a LAN segment that is at the end of a bridged LAN or is attached to an end node.

CLI REFERENCES

- "Spanning Tree Commands" on page 743

PARAMETERS

These parameters are displayed:

- **Admin Edge Port** – Since end nodes **cannot** cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device. (Default: Disabled)

  - **Enabled** – Manually configures a port as an Edge Port.
  - **Disabled** – Disables the Edge Port setting.
  - **Auto** – The port will be automatically configured as an edge port if the edge delay time expires without receiving any RSTP or MSTP BPDUs. Note that edge delay time (802.1D-2004 17.20.4) equals the protocol migration time if a port's link type is point-to-point (which is 3 seconds as defined in IEEE 802.3D-2004 17.20.4); otherwise it equals the spanning tree's maximum age for configuration messages (see maximum age under "Configuring Global Settings for STA").

  An interface cannot function as an edge port under the following conditions:

  - If spanning tree mode is set to STP (page 305), edge-port mode can be manually enabled or set to auto, but will have no effect.
  - If loopback detection is enabled (page 302) and a loopback BPDU is detected, the interface cannot function as an edge port until the loopback state is released.
  - If an interface is in forwarding state and its role changes, the interface cannot continue to function as an edge port even if the edge delay time has expired.
  - If the port does not receive any BPDUs after the edge delay timer expires, its role changes to designated port and it immediately

enters forwarding state (see "Displaying Interface Settings for STA").

- **BPDU Guard** – This feature protects edge ports from receiving BPDUs. It prevents loops by shutting down an edge port when a BPDU is received instead of putting it into the spanning tree discarding state. In a valid configuration, configured edge ports should not receive BPDUs. If an edge port receives a BPDU an invalid configuration exists, such as a connection to an unauthorized device. The BPDU guard feature provides a secure response to invalid configurations because an administrator must manually enable the port. (Default: Disabled)

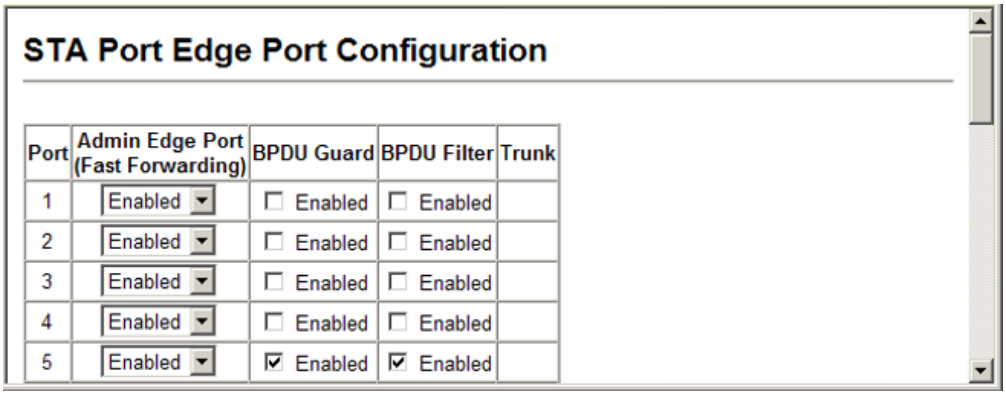
- **BPDU Filter** – BPDU filtering allows you to avoid transmitting BPDUs on configured edge ports that are connected to end nodes. By default, STA sends BPDUs to all ports regardless of whether administrative edge is enabled on a port. BDPU filtering is configured on a per-port basis. (Default: Disabled)

WEB INTERFACE

To configure interface settings for STA:

1. Click Spanning Tree, STA, Port Edge Port Configuration or Trunk Edge Port Configuration.
2. Modify any of the required attributes.
3. Click Apply.

Figure 143: Configuring Edge Port Settings for STA



CONFIGURING MULTIPLE SPANNING TREES

Use the Spanning Tree > MSTP > VLAN Configuration page to create an MSTP instance, or to add VLAN groups to an MSTP instance.

CLI REFERENCES

- "Spanning Tree Commands" on page 743

COMMAND USAGE

MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.

By default all VLANs are assigned to the Internal Spanning Tree (MST Instance 0) that connects all bridges and LANs within the MST region. This switch supports up to 9 instances. You should try to group VLANs which cover the same general area of your network. However, remember that you must configure all bridges within the same MSTI Region (page 305) with the same set of instances, and the same instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each MSTI region as a single node, connecting all regions to the Common Spanning Tree.

To use multiple spanning trees:

1. Set the spanning tree type to MSTP (page 305).
2. Enter the spanning tree priority for the selected MST instance on the Spanning Tree > MSTP (Configure Global - Add) page.
3. Add the VLANs that will share this MSTI on the Spanning Tree > MSTP (Configure Global - Add Member) page.

NOTE: All VLANs are automatically added to the IST (Instance 0).

To ensure that the MSTI maintains connectivity across the network, you must configure a related set of bridges with the same MSTI settings.

PARAMETERS

These parameters are displayed:

- **MST Instance ID** – Instance identifier to configure. (Default: 0)
- **Priority** – The priority of a spanning tree instance. (Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440; Default: 32768)
- **VLANs in MST Instance** – VLANs assigned to this instance.

- **MST ID** – Instance identifier to configure. (Range: 0-4094)
- **VLAN ID** – VLAN to assign to this MST instance. (Range: 1-4094)

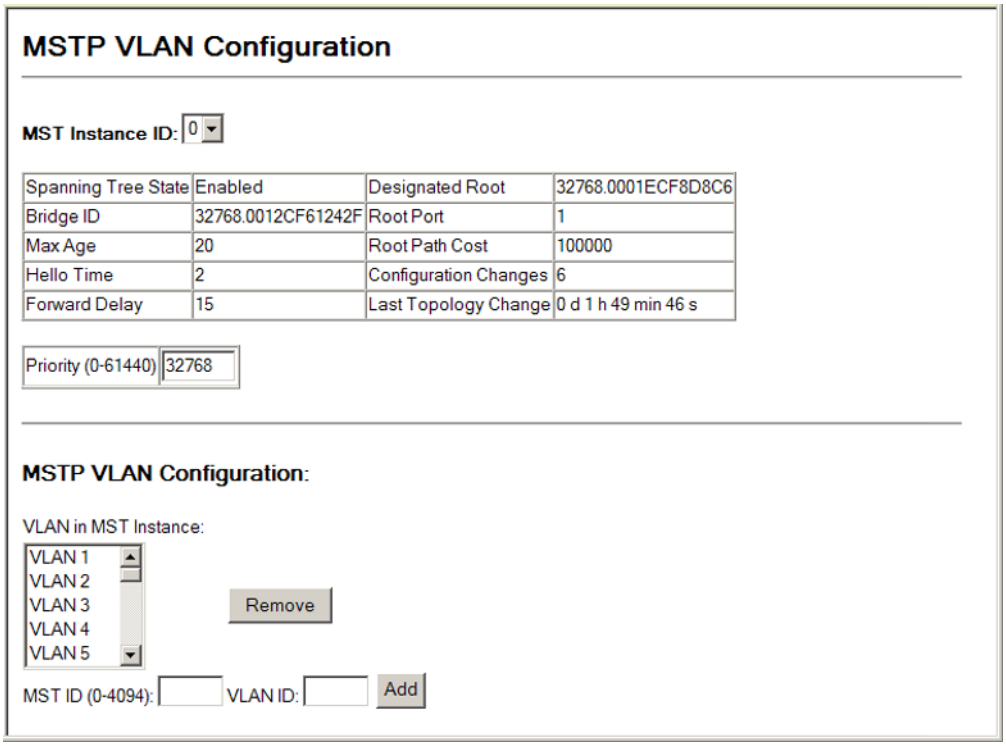
The other global attributes are described under "Displaying Global Settings for STA."

WEB INTERFACE

To create instances for MSTP:

1. Click Spanning Tree, MSTP, VLAN Configuration.
2. Select an instance identifier from the list, set the instance priority, and click Apply.
3. To add the VLAN members to an MSTI instance, enter the instance identifier, the VLAN identifier, and click Add.

Figure 144: Creating an MST Instance



DISPLAYING INTERFACE SETTINGS FOR MSTP

Use the Spanning Tree > MSTP > Port Information or Trunk Information page to display the current status of ports and trunks in the selected MST instance.

CLI REFERENCES

- "show spanning-tree" on page 768

PARAMETERS

These parameters are displayed:

- **MST Instance ID** – Instance identifier to configure. (Range: 0-4094; Default: 0)

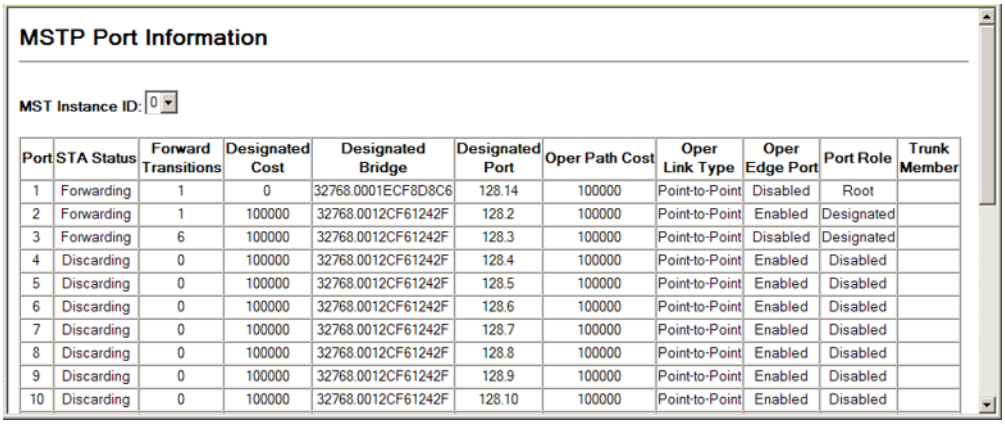
The other attributes are described under "Displaying Interface Settings for STA."

WEB INTERFACE

To create instances for MSTP:

1. Click Spanning Tree, MSTP, Port Information or Trunk Information.
2. Select the required MST instance to display the current spanning tree values.

Figure 145: Displaying MSTP Interface Settings



Port	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Forwarding	1	0	32768.0001ECF8D8C6	128.14	100000	Point-to-Point	Disabled	Root	
2	Forwarding	1	100000	32768.0012CF61242F	128.2	100000	Point-to-Point	Enabled	Designated	
3	Forwarding	6	100000	32768.0012CF61242F	128.3	100000	Point-to-Point	Disabled	Designated	
4	Discarding	0	100000	32768.0012CF61242F	128.4	100000	Point-to-Point	Enabled	Disabled	
5	Discarding	0	100000	32768.0012CF61242F	128.5	100000	Point-to-Point	Enabled	Disabled	
6	Discarding	0	100000	32768.0012CF61242F	128.6	100000	Point-to-Point	Enabled	Disabled	
7	Discarding	0	100000	32768.0012CF61242F	128.7	100000	Point-to-Point	Enabled	Disabled	
8	Discarding	0	100000	32768.0012CF61242F	128.8	100000	Point-to-Point	Enabled	Disabled	
9	Discarding	0	100000	32768.0012CF61242F	128.9	100000	Point-to-Point	Enabled	Disabled	
10	Discarding	0	100000	32768.0012CF61242F	128.10	100000	Point-to-Point	Enabled	Disabled	

CONFIGURING INTERFACE SETTINGS FOR MSTP

Use the Spanning Tree > MSTP > Port Configuration or Trunk Configuration page to configure the STA interface settings for an MST instance.

CLI REFERENCES

- "Spanning Tree Commands" on page 743

PARAMETERS

These parameters are displayed:

- **MST Instance ID** – Instance identifier to configure. (Default: 0)
- *Interface* – Displays a list of ports or trunks.
- **STA State** – Displays the current state of this interface within the Spanning Tree. (See "Displaying Interface Settings for STA" for additional information.)
  - **Discarding** – Port receives STA configuration messages, but does not forward packets.
  - **Learning** – Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** – Port forwards packets, and continues learning addresses.
- **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. (Default: 128; Range: 0-240, in steps of 16)
- **Admin MST Path Cost** – This parameter is used by the MSTP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to short (page 3-63), the maximum path cost is 65,535.

  By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

The recommended range is listed in Table 22 on page 313.
The recommended path cost is listed in Table 23 on page 313.
The default path costs are listed in Table 24 on page 313.

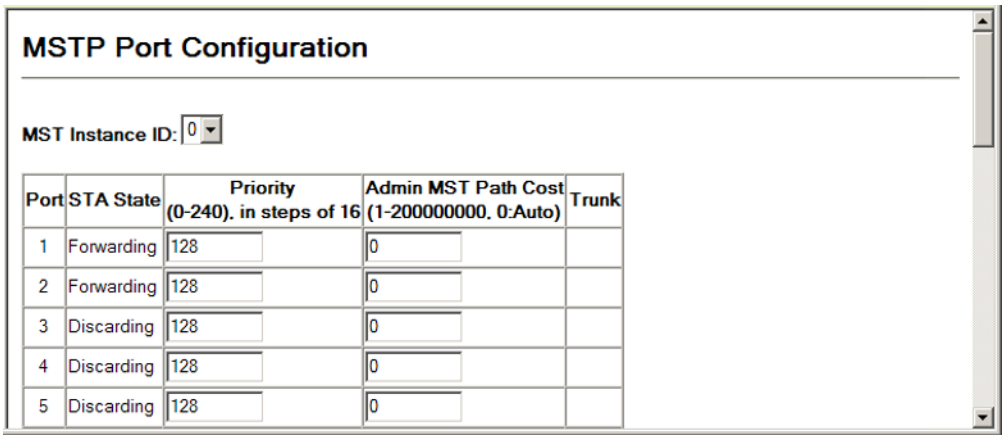
- **Trunk** – Indicates if a port is a member of a trunk. (MSTP Port Configuration only)

WEB INTERFACE

To configure MSTP parameters for a port or trunk:

1. Click Spanning Tree, MSTP, Port Configuration.
2. Enter the priority and path cost for an interface
3. Click Apply.

Figure 146: Configuring MSTP Interface Settings



11 LAYER 2 PROTOCOL TUNNELING

This chapter describes the following basic topics:

- Configuring the Tunnel Address – Configures the destination address for BPDU tunneling.
- Enabling L2PT Tunneling – Enables Layer 2 Protocol Tunneling for the specified interface.

OVERVIEW

L2 Protocol Tunnelling (L2PT) is used to tunnel local network protocols across a service provider's network. This switch currently supports tunneling for the Spanning Tree protocol, passing BPDUs across a service provider's network without any changes, and thereby combining remote network segments into a single spanning tree domain. As implemented on this switch, L2PT allows a port which is not participating in the spanning tree (such as an uplink port to the service provider's network) to forward BPDU packets to other ports instead of discarding these packets or attempting to process them.

CONFIGURING THE TUNNEL ADDRESS FOR UPLINK TRAFFIC

Use the L2 Protocol Tunnel Configuration page to set the destination address assigned to spanning tree protocol packets entering the service provider's network.

CLI REFERENCES

- "l2protocol-tunnel tunnel-dmac" on page 819

COMMAND USAGE

- When L2 Protocol Tunneling is enabled, the switch encapsulates spanning tree protocol packets entering ingress ports on the service provider's edge switch, replacing the destination MAC address with a proprietary MAC address for the spanning tree protocol (i.e., 10-12-CF-00-00-02) or a user-defined address.
- When a tunneled BPDU enters the tunnel egress port attached to a remote portion of the customer's network, the switch decapsulates these packets, restores the proper protocol and MAC address information, and then floods them onto the same VLANs at the customer's remote site.

PARAMETERS

These parameters are displayed:

- **Tunnel Address** - When a BPDU is received at a tunnel port, the packet is encapsulated, and the destination MAC address is changed to the proprietary tunnel address (01-12-CF-.00-00-02) or a user-specified address. (Default: 01-12-CF-.00-00-02)

  The tunnel address can be any multicast address, except for the following:

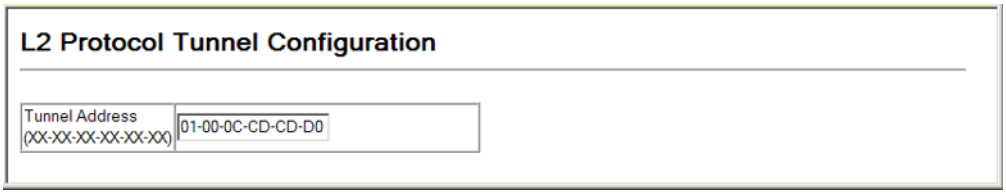
  - IPv4 multicast addresses (with prefix 01-00-5E).
  - IPv6 multicast addresses (with prefix 33-33-33).
  - Addresses used by the spanning tree protocol.

WEB INTERFACE

To configure the tunnel address for L2PT:

1. Click L2 Protocol Tunnel, Configuration.
2. Enter the tunnel address required by your service provider.
3. Click Apply.

Figure 147: Setting the Layer 2 Protocol Tunnel Address



ENABLING TUNNELING FOR INTERFACES

Use the L2 Protocol Tunnel Port or Trunk Configuration page to enable Layer 2 Protocol Tunneling (L2PT) for the spanning tree protocol on the specified uplink port.

CLI REFERENCES

- "switchport l2protocol-tunnel" on page 820

COMMAND USAGE

- When L2PT is not used, spanning tree protocol packets are flooded to 802.1Q access ports on the same edge switch, but filtered from 802.1Q tunnel ports. This creates disconnected protocol domains in the customer's network.
- L2PT can be used to pass BPDU packets belonging to the same customer transparently across a service provider's network. In this

way, normally segregated network segments can be configured to function inside a common protocol domain.

- L2PT encapsulates protocol packets entering ingress ports on the service provider's edge switch, replacing the destination MAC address with a proprietary MAC address for the spanning tree protocol (i.e., 10-12-CF-00-00-02) or a user-defined address. All intermediate switches carrying this traffic across the service provider's network treat these encapsulated packets in the same way as normal data, forwarding them across to the tunnel's egress port. The egress port decapsulates these packets, restores the proper protocol and MAC address information, and then floods them onto the same VLANs at the customer's remote site (via all of the appropriate tunnel ports and access ports[11] connected to the same metro VLAN).

- For L2PT to function properly, QinQ must be enabled on the switch (see "Enabling QinQ Tunneling on the Switch" on page 343), and the interface configured to 802.1Q tunnel mode (see "Adding an Interface to a QinQ Tunnel" on page 344).

PARAMETERS

These parameters are displayed:

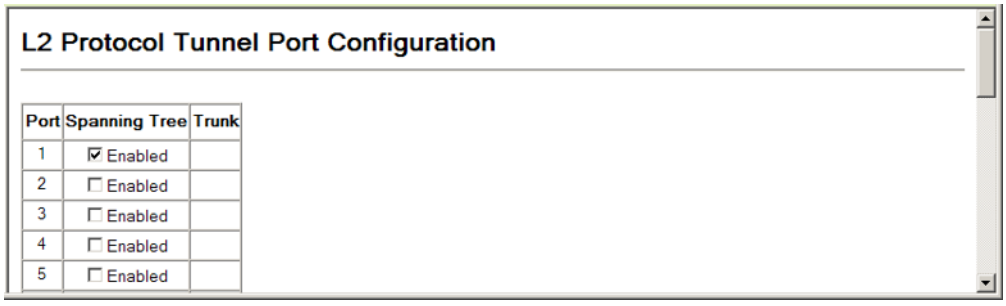
- **Spanning Tree** - Spanning Tree (STP, RSTP and MSTP)

WEB INTERFACE

To enable tunneling on an interface:

1. Click L2 Protocol Tunnel, Port Configuration or Trunk Configuration.
2. Enable protocol tunneling for a port or trunk.
3. Click Apply.

Figure 148: Enabling Layer 2 Protocol Tunneling



11. Access ports in this context are 802.1Q trunk ports.

12 VLAN CONFIGURATION

This chapter includes the following topics:

- IEEE 802.1Q VLANs – Configures static and dynamic VLANs.
- IEEE 802.1Q Tunneling – Configures QinQ tunneling to maintain customer-specific VLAN and Layer 2 protocol configurations across a service provider network, even when different customers use the same internal VLAN IDs.
- Traffic Segmentation – Configures the uplinks and down links to a segmented group of ports.
- Private VLANs – Configures private VLANs, using primary for unrestricted upstream access and community groups which are restricted to other local group members or to the ports in the associated primary group.
- Protocol VLANs – Configures VLAN groups based on specified protocols.
- VLAN Mirroring – Mirrors traffic from one or more source VLANs to a target port.
- IP Subnet VLANs – Maps untagged ingress frames to a specified VLAN if the source address is found in the IP subnet-to-VLAN mapping table.
- MAC-based VLANs – Maps untagged ingress frames to a specified VLAN if the source MAC address is found in the IP MAC address-to-VLAN mapping table.

IEEE 802.1Q VLANs

In large networks, routers are used to isolate broadcast traffic for each subnet into separate domains. This switch provides a similar service at Layer 2 by using VLANs to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections.

VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as video conferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

This switch supports the following VLAN features:

- Up to 255 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GVRP protocol
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

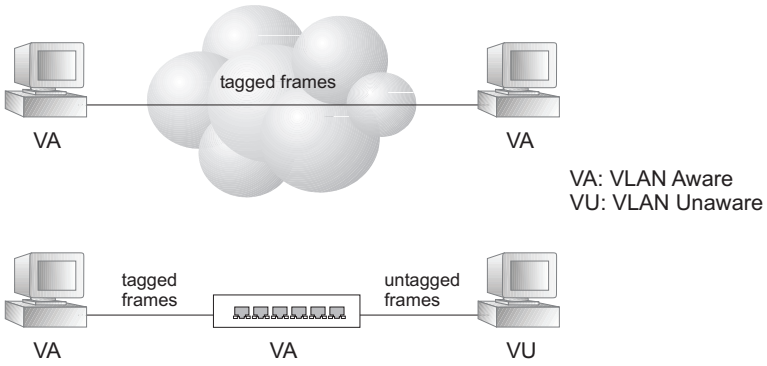
NOTE: The switch allows 255 user-manageable VLANs. One extra, unmanageable VLAN (VLAN ID 4093) is maintained for IP clustering.

Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

NOTE: VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing it on to any end-node host that does not support VLAN tagging.

Figure 149: VLAN Compliant and VLAN Non-compliant Devices



VLAN Classification – When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the default VLAN ID of the receiving port). But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

Port Overlapping – Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by enabled routing on this switch.

Untagged VLANs – Untagged VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets. However, you should use IEEE 802.3 tagged VLANs with GVRP whenever possible to fully automate VLAN registration.

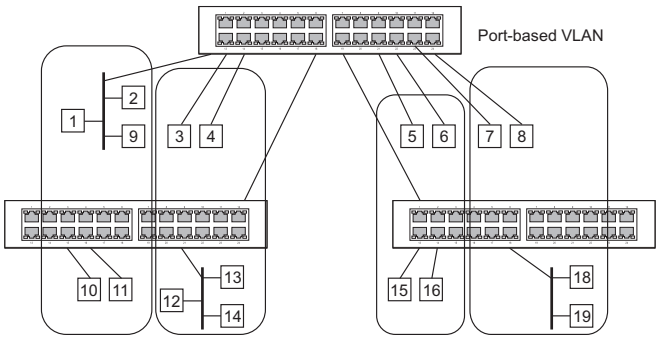
Automatic VLAN Registration – GVRP (GARP VLAN Registration Protocol) defines a system whereby the switch can automatically learn the VLANs to which each end station should be assigned. If an end station (or its network adapter) supports the IEEE 802.1Q VLAN protocol, it can be configured to broadcast a message to your network indicating the VLAN groups it wants to join. When this switch receives these messages, it will automatically place the receiving port in the specified VLANs, and then forward the message to all other ports. When the message arrives at another switch that supports GVRP, it will also place the receiving port in the specified VLANs, and pass the message on to all other ports. VLAN requirements are propagated in this way throughout the network. This allows GVRP-compliant devices to be automatically configured for VLAN groups based solely on end station requests.

To implement GVRP in a network, first add the host devices to the required VLANs (using the operating system or other application software), so that these VLANs can be propagated onto the network. For both the edge switches attached directly to these hosts, and core switches in the network, enable GVRP on the links between these devices. You should also determine security boundaries in the network and disable GVRP on the

boundary ports to prevent advertisements from being propagated, or forbid those ports from joining restricted VLANs.

NOTE: If you have host devices that do not support GVRP, you should configure static or untagged VLANs for the switch ports connected to these devices (as described in "Adding Static Members to VLANs"). But you can still enable GVRP on these edge switches, as well as on the core switches in the network.

Figure 150: Using GVRP



Forwarding Tagged/Untagged Frames

If you want to create a small port-based VLAN for devices attached directly to a single switch, you can assign ports to the same untagged VLAN. However, to participate in a VLAN group that crosses several switches, you should create a VLAN for that group and enable tagging on all ports.

Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is therefore capable of passing tagged or untagged frames. When forwarding a frame from this switch along a path that contains any VLAN-aware devices, the switch should include VLAN tags. When forwarding a frame from this switch along a path that does not contain any VLAN-aware devices (including the destination host), the switch must first strip off the VLAN tag before forwarding the frame. When the switch receives a tagged frame, it will pass this frame onto the VLAN(s) indicated by the frame tag. However, when this switch receives an untagged frame from a VLAN-unaware device, it first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID.

CONFIGURING GLOBAL SETTINGS FOR DYNAMIC VLAN REGISTRATION

Use the VLAN > 802.1Q VLAN > GVRP Status page to enable GVRP globally on the switch.

CLI REFERENCES

- "GVRP and Bridge Extension Commands" on page 800

PARAMETERS

These parameters are displayed:

- **GVRP** – GVRP defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. VLANs are dynamically configured based on join messages issued by host devices and propagated throughout the network. GVRP must be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch. (Default: Disabled)

WEB INTERFACE

To configure GVRP on the switch:

1. Click VLAN, 802.1Q VLAN, GVRP Status.
2. Enable or disable GVRP.
3. Click Apply.

Figure 151: Configuring Global Status of GVRP

DISPLAYING BASIC VLAN INFORMATION

Use the VLAN > 802.1Q VLAN > Basic Information page to display basic information on the VLAN type supported by the switch.

CLI REFERENCES

- "show bridge-ext" on page 803

PARAMETERS

These parameters are displayed:

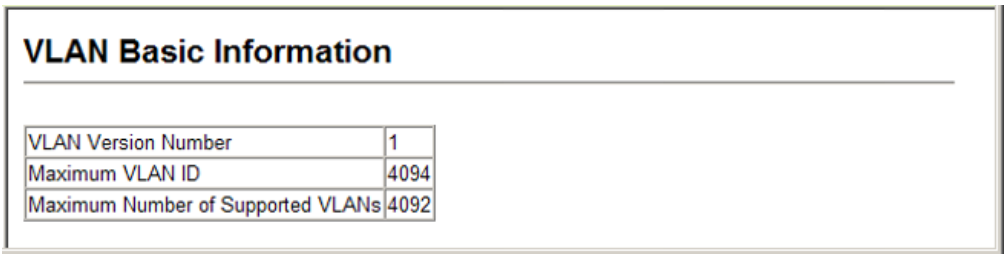
- **VLAN Version Number** – The VLAN version used by this switch as specified in the IEEE 802.1Q standard.
- **Maximum VLAN ID** – Maximum VLAN ID recognized by this switch.
- **Maximum Number of Supported VLANs** – Maximum number of VLANs that can be configured on this switch.

WEB INTERFACE

To display basic information on the VLAN type supported by the switch:

1. Click VLAN, 802.1Q VLAN, Basic Information.

Figure 152: Displaying Basic VLAN Information



DISPLAYING CURRENT VLANS

Use the VLAN > 802.1Q VLAN > Current Table page to shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. However, if you just want to create a small port-based VLAN for one or two switches, you can disable tagging.

CLI REFERENCES

- "show vlan" on page 813

PARAMETERS

These parameters are displayed:

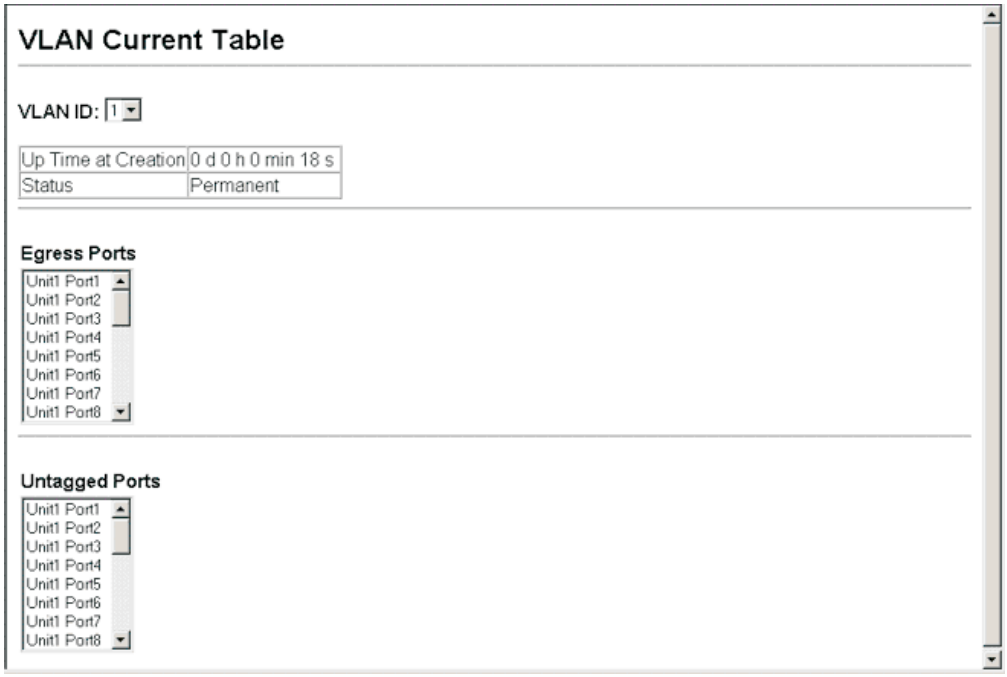
- **VLAN ID** – ID of configured VLAN (1-4094).
- **Up Time at Creation** – Time this VLAN was created (i.e., System Up Time).
- **Status** – Shows how this VLAN was added to the switch.
  - **Dynamic GVRP**: Automatically learned via GVRP.
  - **Permanent**: Added as a static entry.
- **Egress Ports** – Shows all the VLAN port members.
- **Untagged Ports** – Shows the untagged VLAN port members.

WEB INTERFACE

To shows the current port members of each VLAN:

1. Click VLAN, 802.1Q VLAN, Current Table.

Figure 153: Displaying Current VLANs



CONFIGURING VLAN GROUPS

Use the VLAN > 802.1Q VLAN > Static List page to create or remove VLAN groups. To propagate information about VLAN groups used on this switch to external network devices, you must specify a VLAN ID for each of these groups.

CLI REFERENCES

- "Editing VLAN Groups" on page 804

PARAMETERS

These parameters are displayed:

- **VLAN ID** – ID of VLAN or range of VLANs (1-4094).

  Up to 255 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.

- **VLAN Name** – Name of the VLAN (1-128 characters, no spaces).

- **Status** – Enables or disables the specified VLAN.

- **Add** – Adds a new VLAN group to the current list.

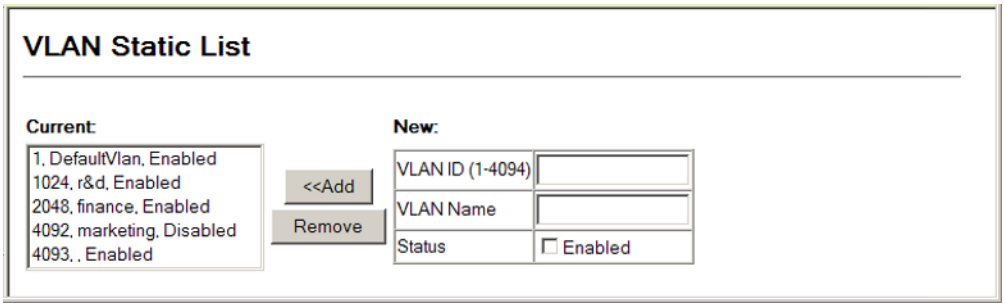
- **Remove** – Removes a VLAN group from the current list. If any port is assigned to this group as untagged, it will be reassigned to VLAN group 1 as untagged.

WEB INTERFACE

To create static VLANs:

1. Click VLAN, 802.1Q VLAN, Static List.
2. Enter the VLAN ID and VLAN name, mark the Enable checkbox to activate the VLAN.
3. Click Add.

Figure 154: Creating Static VLANs



ADDING STATIC MEMBERS TO VLANS

Use the VLAN > 802.1Q VLAN > Static Table page to configure port members for the selected VLAN index. Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices, or untagged they are not connected to any VLAN-aware devices. Or configure a port as forbidden to prevent the switch from automatically adding it to a VLAN via the GVRP protocol.

CLI REFERENCES

- "Configuring VLAN Interfaces" on page 806
- "Displaying VLAN Information" on page 813

PARAMETERS

These parameters are displayed:

- **VLAN ID** – ID of configured VLAN (1-4094).
- **VLAN Name** – Name of the VLAN (1 to 100 characters).
- **Status** – Enables or disables the specified VLAN.
- **Port** – Port Identifier. (Range: 1-28/52)
- **Trunk** – Trunk Identifier. (Range: 1-8)

- **Tagged**: Interface is a member of the VLAN. All packets transmitted by the port will be tagged, that is, carry a tag and therefore carry VLAN or CoS information.
- **Untagged**: Interface is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a tag and therefore not carry VLAN or CoS information. Note that an interface must be assigned to at least one group as an untagged port.
- **Forbidden**: Interface is forbidden from automatically joining the VLAN via GVRP. For more information, see "Automatic VLAN Registration" on page 329.
- **None**: Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.

NOTE: VLAN 1 is the default untagged VLAN containing all ports on the switch using Access mode.

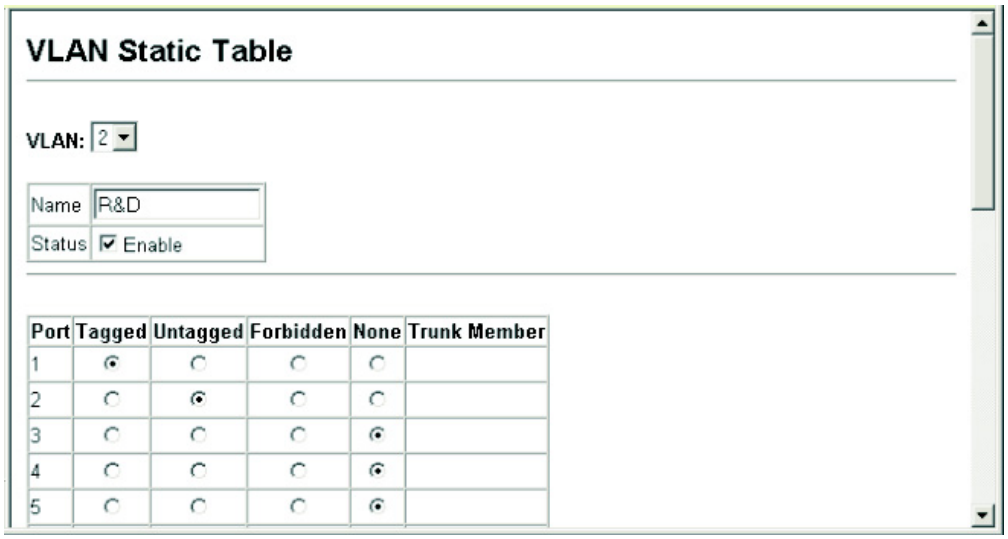
- **Trunk Member** – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.

WEB INTERFACE

To configure port members for the selected VLAN:

1. Click VLAN, 802.1Q VLAN, Static Table.
2. Select a VLAN ID from the scroll-down list. Modify the VLAN name and status if required. Select the membership type by marking the appropriate radio button in the list of ports or trunks.
3. Click Apply.

Figure 155: Adding Static Members to VLANs



ADDING VLAN GROUPS TO INTERFACES

Use the VLAN > 802.1Q > Static Membership by Port page to assign VLAN groups to the selected interface as a tagged member.

CLI REFERENCES

- "switchport allowed vlan" on page 808
- "Displaying VLAN Information" on page 813

PARAMETERS

These parameters are displayed:

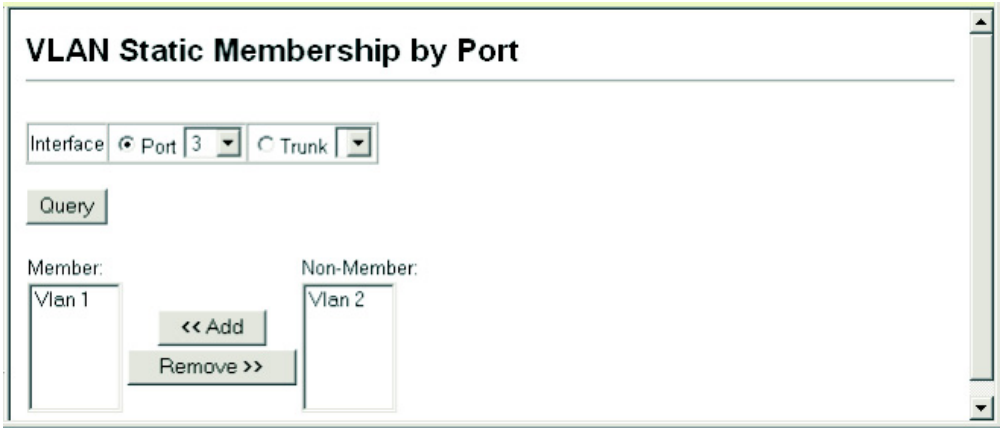
- **Interface** – Port or trunk identifier.
- **Member** – VLANs for which the selected interface is a tagged member.
- **Non-Member** – VLANs for which the selected interface is not a tagged member.

WEB INTERFACE

To assign VLAN groups to the selected interface as a tagged member:

1. Click VLAN, 802.1Q VLAN, Static Membership by Port.
2. Select an interface from the scroll-down box (Port or Trunk), and click Query to display membership information for the interface.
3. Select a VLAN ID, and then click Add to add the interface as a tagged member, or click Remove to remove the interface.

Figure 156: Adding VLAN Groups to an Interface



CONFIGURING VLAN ATTRIBUTES FOR INTERFACES

Use the VLAN > 802.1Q VLAN > Port Configuration or Trunk Configuration to configure VLAN attributes for specific interfaces, including the default VLAN identifier (PVID), accepted frame types, ingress filtering, GVRP status, GARP timers, and mode of operation (Hybrid, 1Q Trunk or Access port); or to enable GVRP and adjust the protocol timers per interface

CLI REFERENCES

- "Configuring VLAN Interfaces" on page 806
- "Displaying VLAN Information" on page 813

PARAMETERS

These parameters are displayed:

- **PVID** – VLAN ID assigned to untagged frames received on the interface. (Default: 1)

  When using Access mode, and an interface is assigned to a new VLAN, its PVID is automatically set to the identifier for that VLAN. When using Hybrid mode, the PVID for an interface can be set to any VLAN for which it is an untagged member.

- **Acceptable Frame Type** – Sets the interface to accept all frame types, including tagged or untagged frames, or only tagged frames. When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN. (Options: All, Tagged; Default: All)

- **Ingress Filtering** – Determines how to process frames tagged for VLANs for which the ingress port is not a member. (Default: Disabled)

  - Ingress filtering only affects tagged frames.
  - If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).

- If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
- Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STP. However, they do affect VLAN dependent BPDU frames, such as GMRP.

- **Mode** – Indicates VLAN membership mode for an interface. (Default: Hybrid)
  - **Access** - Sets the port to operate as an untagged interface. The port transmits and receives untagged frames on a single VLAN only.

    Access mode is mutually exclusive with VLAN trunking (see "VLAN Trunking"). If VLAN trunking is enabled on an interface, then that interface cannot be set to access mode, and vice versa.
  - **Hybrid** – Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.
  - **1Q Trunk** – Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. Note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are also transmitted as tagged frames.
- **GVRP Status** – Enables/disables GVRP for the interface. GVRP must be globally enabled for the switch before this setting can take effect (see page 331). When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. (Default: Disabled)

GARP Timers – Group Address Registration Protocol is used by GVRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GVRP registration/deregistration. The following GARP timer settings must follow this rule:
2 x (join timer) < leave timer < leaveAll timer

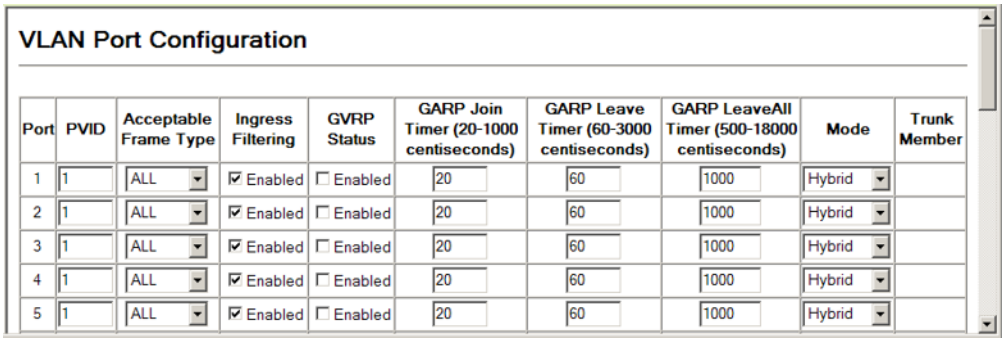
- **GARP Join** – The interval between transmitting requests/queries to participate in a VLAN group. (Range: 20-1000 centiseconds; Default: 20)
- **GARP Leave** – The interval a port waits before leaving a VLAN group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group. (Range: 60-3000 centiseconds; Default: 60)
- **GARP LeaveAll** – The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group. (Range: 500-18000 centiseconds; Default: 1000)

WEB INTERFACE

To to configure VLAN attributes for specific interfaces:

1. Click VLAN, 802.1Q VLAN, Port Configuration or Trunk Configuration.
2. Enter in the required settings for each interface.
3. Click Apply.

Figure 157: Adding VLAN Groups to an Interface



IEEE 802.1Q TUNNELING

IEEE 802.1Q Tunneling (QinQ) is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting Service Provider VLAN (SPVLAN) tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4096.

QinQ tunneling uses a single Service Provider VLAN (SPVLAN) for customers who have multiple VLANs. Customer VLAN IDs are preserved and traffic from different customers is segregated within the service provider's network even when they use the same customer-specific VLAN IDs. QinQ tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy, preserving the customer's original tagged packets, and adding SPVLAN tags to each frame (also called double tagging).

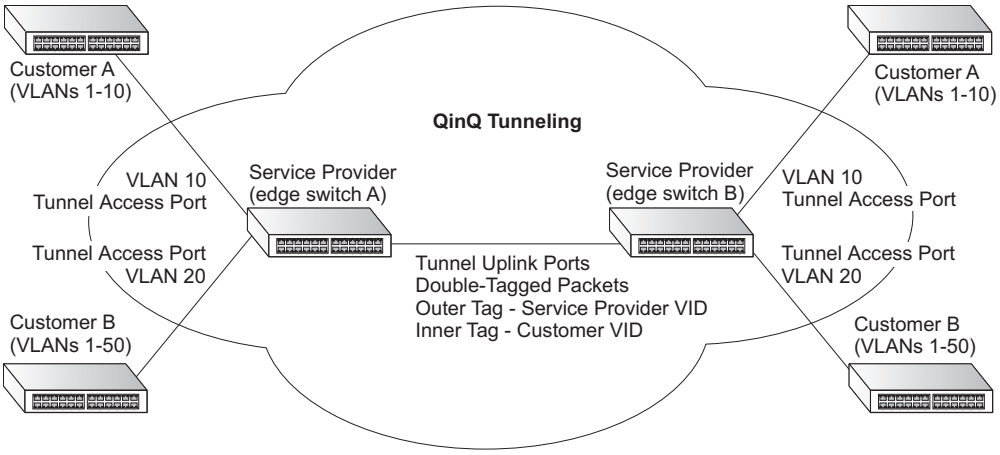
A port configured to support QinQ tunneling must be set to tunnel port mode. The Service Provider VLAN (SPVLAN) ID for the specific customer must be assigned to the QinQ tunnel access port on the edge switch where the customer traffic enters the service provider's network. Each customer

requires a separate SPVLAN, but this VLAN supports all of the customer's internal VLANs. The QinQ tunnel uplink port that passes traffic from the edge switch into the service provider's metro network must also be added to this SPVLAN. The uplink port can be added to multiple SPVLANs to carry inbound traffic for different customers onto the service provider's network.

When a double-tagged packet enters another trunk port in an intermediate or core switch in the service provider's network, the outer tag is stripped for packet processing. When the packet exits another trunk port on the same core switch, the same SPVLAN tag is again added to the packet.

When a packet enters the trunk port on the service provider's egress switch, the outer tag is again stripped for packet processing. However, the SPVLAN tag is not added when it is sent out the tunnel access port on the edge switch into the customer's network. The packet is sent as a normal IEEE 802.1Q-tagged frame, preserving the original VLAN numbers used in the customer's network.

Figure 158: QinQ Operational Concept



Layer 2 Flow for Packets Coming into a Tunnel Access Port

A QinQ tunnel port may receive either tagged or untagged packets. No matter how many tags the incoming packet has, it is treated as tagged packet.

The ingress process does source and destination lookups. If both lookups are successful, the ingress process writes the packet to memory. Then the egress process transmits the packet. Packets entering a QinQ tunnel port are processed in the following manner:

1. New SPVLAN tags are added to all incoming packets, no matter how many tags they already have. The ingress process constructs and inserts the outer tag (SPVLAN) into the packet based on the default VLAN ID and Tag Protocol Identifier (TPID, that is, the ether-type of the tag). This outer tag is used for learning and switching packets. The priority of the inner tag is copied to the outer tag if it is a tagged or priority tagged packet.

2. After successful source and destination lookup, the ingress process sends the packet to the switching process with two tags. If the incoming packet is untagged, the outer tag is an SPVLAN tag, and the inner tag is a dummy tag (8100 0000). If the incoming packet is tagged, the outer tag is an SPVLAN tag, and the inner tag is a CVLAN tag.

3. After packet classification through the switching process, the packet is written to memory with one tag (an outer tag) or with two tags (both an outer tag and inner tag).

4. The switch sends the packet to the proper egress port.

5. If the egress port is an untagged member of the SPVLAN, the outer tag will be stripped. If it is a tagged member, the outgoing packets will have two tags.

Layer 2 Flow for Packets Coming into a Tunnel Uplink Port

An uplink port receives one of the following packets:

- Untagged
- One tag (CVLAN or SPVLAN)
- Double tag (CVLAN + SPVLAN)

The ingress process does source and destination lookups. If both lookups are successful, the ingress process writes the packet to memory. Then the egress process transmits the packet. Packets entering a QinQ uplink port are processed in the following manner:

1. If incoming packets are untagged, the PVID VLAN native tag is added.

2. If the ether-type of an incoming packet (single or double tagged) is not equal to the TPID of the uplink port, the VLAN tag is determined to be a Customer VLAN (CVLAN) tag. The uplink port's PVID VLAN native tag is added to the packet. This outer tag is used for learning and switching packets within the service provider's network. The TPID must be configured on a per port basis, and the verification cannot be disabled.

3. If the ether-type of an incoming packet (single or double tagged) is equal to the TPID of the uplink port, no new VLAN tag is added. If the uplink port is not the member of the outer VLAN of the incoming packets, the packet will be dropped when ingress filtering is enabled. If ingress filtering is not enabled, the packet will still be forwarded. If the VLAN is not listed in the VLAN table, the packet will be dropped.

4. After successful source and destination lookups, the packet is double tagged. The switch uses the TPID of 0x8100 to indicate that an incoming packet is double-tagged. If the outer tag of an incoming double-tagged packet is equal to the port TPID and the inner tag is 0x8100, it is treated as a double-tagged packet. If a single-tagged packet has 0x8100 as its TPID, and port TPID is not 0x8100, a new VLAN tag is added and it is also treated as double-tagged packet.

5. If the destination address lookup fails, the packet is sent to all member ports of the outer tag's VLAN.

6. After packet classification, the packet is written to memory for processing as a single-tagged or double-tagged packet.

7. The switch sends the packet to the proper egress port.

8. If the egress port is an untagged member of the SPVLAN, the outer tag will be stripped. If it is a tagged member, the outgoing packet will have two tags.

Configuration Limitations for QinQ

- The native VLAN of uplink ports should not be used as the SPVLAN. If the SPVLAN is the uplink port's native VLAN, the uplink port must be an untagged member of the SPVLAN. Then the outer SPVLAN tag will be stripped when the packets are sent out. Another reason is that it causes non-customer packets to be forwarded to the SPVLAN.

- Static trunk port groups are compatible with QinQ tunnel ports as long as the QinQ configuration is consistent within a trunk port group.

- The native VLAN (VLAN 1) is not normally added to transmitted frames. Avoid using VLAN 1 as an SPVLAN tag for customer traffic to reduce the risk of misconfiguration. Instead, use VLAN 1 as a management VLAN instead of a data VLAN in the service provider network.

- There are some inherent incompatibilities between Layer 2 and Layer 3 switching:
  - Tunnel ports do not support IP Access Control Lists.
  - Layer 3 Quality of Service (QoS) and other QoS features containing Layer 3 information are not supported on tunnel ports.
  - Spanning tree bridge protocol data unit (BPDU) filtering is automatically disabled on a tunnel port.

General Configuration Guidelines for QinQ

1. Enable Tunnel Status, and set the Tag Protocol Identifier (TPID) value of the tunnel access port (in the Ethernet Type field. This step is required if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The default ethertype value is 0x8100. (See "Enabling QinQ Tunneling on the Switch.")

2. Create a Service Provider VLAN, also referred to as an SPVLAN (see "Configuring VLAN Groups").

3. Configure the QinQ tunnel access port to Tunnel mode (see "Adding an Interface to a QinQ Tunnel").

4. Configure the QinQ tunnel access port to join the SPVLAN as an untagged member (see "Adding Static Members to VLANs").

5. Configure the SPVLAN ID as the native VID on the QinQ tunnel access port (see "Configuring VLAN Attributes for Interfaces").

6. Configure the QinQ tunnel uplink port to Tunnel Uplink mode (see "Adding an Interface to a QinQ Tunnel").

7. Configure the QinQ tunnel uplink port to join the SPVLAN as a tagged member (see "Adding Static Members to VLANs").

ENABLING QINQ TUNNELING ON THE SWITCH

Use the VLAN > Tunnel (Configure Global) page to configure the switch to operate in IEEE 802.1Q (QinQ) tunneling mode, which is used for passing Layer 2 traffic across a service provider's metropolitan area network. You can also globally set the Tag Protocol Identifier (TPID) value of the tunnel port if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames.

CLI REFERENCES

- "Configuring IEEE 802.1Q Tunneling" on page 814

PARAMETERS

These parameters are displayed:

- **Tunnel Status** – Sets the switch to QinQ mode. (Default: Disabled)

- **Ethernet Type** – The Tag Protocol Identifier (TPID) specifies the ethertype of incoming packets on a tunnel port. (Range: hexadecimal 0800-FFFF; Default: 8100)

  Use this field to set a custom 802.1Q ethertype value. This feature allows the switch to interoperate with third-party switches that do not use the standard 0x8100 ethertype to identify 802.1Q-tagged frames. For example, if 0x1234 is set as the custom 802.1Q ethertype on a trunk port, incoming frames containing that ethertype are assigned to the VLAN contained in the tag following the ethertype field, as they would be with a standard 802.1Q trunk. Frames arriving on the port containing any other ethertype are looked upon as untagged frames, and assigned to the native VLAN of that port.

  All ports on the switch will be set to the same ethertype.

WEB INTERFACE

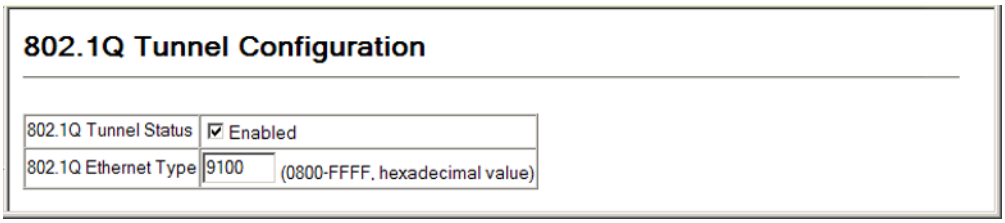
To enable QinQ Tunneling on the switch:

1. Click VLAN, 802.1Q VLAN, Tunnel Configuration.

2. Enable Tunnel Status, and specify the TPID if a client attached to a tunnel port is using a non-standard ethertype to identify 802.1Q tagged frames.

3. Click Apply.

Figure 159: Enabling QinQ Tunneling



ADDING AN INTERFACE TO A QINQ TUNNEL

Follow the guidelines in the preceding section to set up a QinQ tunnel on the switch. Then use the VLAN > 802.1Q VLAN > Tunnel Port Configuration or Tunnel Trunk Configuration page to set the tunnel mode for any participating interface.

CLI REFERENCES

- "Configuring IEEE 802.1Q Tunneling" on page 814

COMMAND USAGE

- Use the 802.1Q Tunnel Configuration page to set the switch to QinQ mode before configuring a tunnel port or tunnel uplink port (see "Enabling QinQ Tunneling on the Switch"). Also set the Tag Protocol Identifier (TPID) value of the tunnel port if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames.

- Then use the Tunnel Port Configuration or Tunnel Trunk Configuration page to set the access interface on the edge switch to Tunnel mode, and set the uplink interface on the switch attached to the service provider network to Tunnel Uplink mode.

PARAMETERS

These parameters are displayed:

- **Interface** – Displays a list of ports or trunks.

- **Port** – Port Identifier. (Range: 1-28/52)

- **Trunk** – Trunk Identifier. (Range: 1-8)

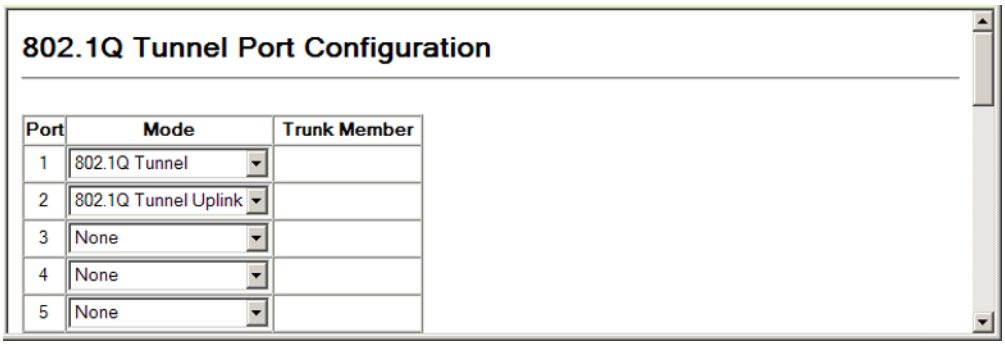
- **Mode** – Sets the VLAN membership mode of the port.
  - **None** – The port operates in its normal VLAN mode. (This is the default.)
  - **802.1Q Tunnel** – Configures QinQ tunneling for a client access port to segregate and preserve customer VLAN IDs for traffic crossing the service provider network.
  - **802.1Q Tunnel Uplink** – Configures QinQ tunneling for an uplink port to another device within the service provider network.
  - **Trunk Member** – Shows if a port is a member or a trunk.

WEB INTERFACE

To add an interface to a QinQ tunnel:

1. Click VLAN, 802.1Q VLAN, Tunnel Port/Trunk Configuration.
2. Set the mode for any tunnel access port to Tunnel and the tunnel uplink port to Tunnel Uplink.
3. Click Apply.

Figure 160: Adding an Interface to a QinQ Tunnel



TRAFFIC SEGMENTATION

If tighter security is required for passing traffic from different clients through downlink ports on the local network and over uplink ports to the service provider, port-based traffic segmentation can be used to isolate traffic for individual client sessions.

Traffic belonging to each client is isolated to the allocated downlink ports. But the switch can be configured to either isolate traffic passing across a client's allocated uplink ports from the uplink ports assigned to other clients, or to also forward traffic through the uplink ports used by other clients, allowing different clients to share access to their uplink ports where security is less likely to be compromised.

CONFIGURING GLOBAL SETTINGS

Use the VLAN > Traffic Segmentation > Status page to enable traffic segmentation, and to block or forward traffic between uplink ports assigned to different client sessions.

CLI REFERENCES

- "Configuring Port-based Traffic Segmentation" on page 821

PARAMETERS

These parameters are displayed:

- **Traffic Segmentation Status** – Enables port-based traffic segmentation. (Default: Disabled)

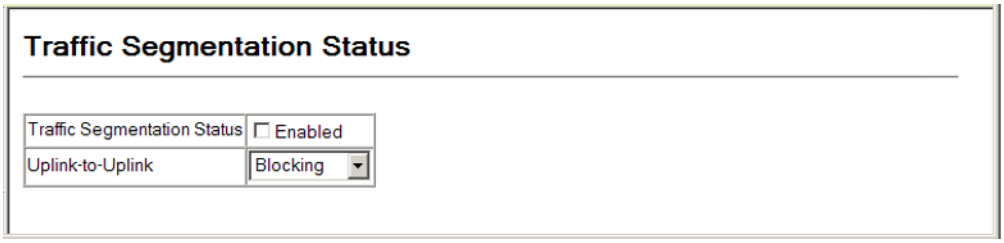
- **Uplink-to-Uplink** – Specifies whether or not traffic can be forwarded between uplink ports assigned to different client sessions. (Default: Blocking)

WEB INTERFACE

To enable traffic segmentation:

1. Click VLAN, Traffic Segmentation, Status.
2. Set the traffic segmentation status or uplink-to-uplink forwarding mode.
3. Click Apply.

Figure 161: Configuring Global Settings for Traffic Segmentation



CONFIGURING UPLINK AND DOWNLINK PORTS

Use the VLAN > Traffic Segmentation > Session Configuration page to create a client session, and assign to service the traffic associated with each session. Ports designated as downlink ports can not communicate with any other ports on the switch except for the uplink ports. Uplink ports can communicate with any other ports on the switch and with any designated downlink ports.

CLI REFERENCES

- "Configuring Port-based Traffic Segmentation" on page 821

PARAMETERS

These parameters are displayed:

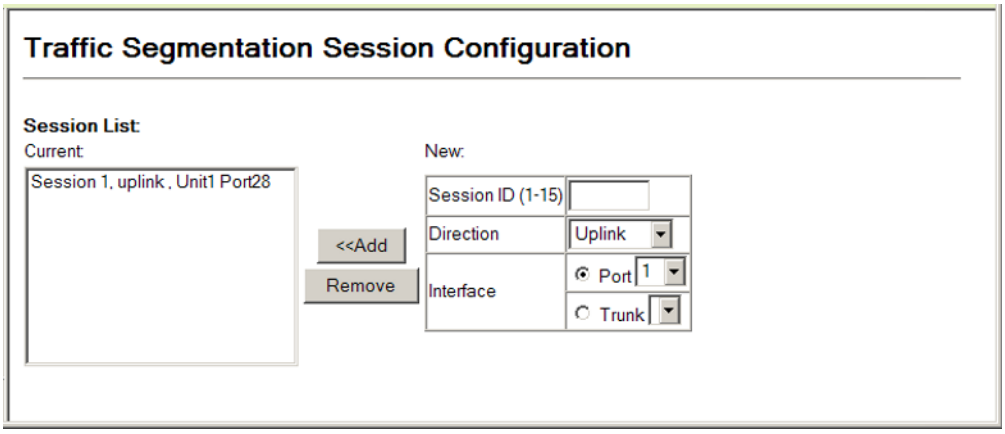
- **Session ID** – Traffic segmentation session. (Range: 1-15)
- **Direction** – Adds an interface to the segmented group by setting the direction to uplink or downlink. (Default: None)
- **Interface** – Displays a list of ports or trunks.
  - **Port** – Port Identifier. (Range: 1-28/52)
  - **Trunk** – Trunk Identifier. (Range: 1-8)

WEB INTERFACE

To configure the members of the traffic segmentation group:

1. Click VLAN, Traffic Segmentation, Session Configuration.
2. Set the session number, specify whether an uplink or downlink is to be used, and select the interface.
3. Click Apply.

Figure 162: Configuring Members for Traffic Segmentation



PRIVATE VLANS

Private VLANs provide port-based security and isolation of local ports contained within different private VLAN groups. This switch supports two types of private VLANs – primary and community groups. A primary VLAN contains promiscuous ports that can communicate with all other ports in the associated private VLAN groups, while a community (or secondary) VLAN contains community ports that can only communicate with other hosts within the community VLAN and with any of the promiscuous ports in the associated primary VLAN. The promiscuous ports are designed to provide open access to an external network such as the Internet, while the community ports provide restricted access to local users.

Multiple primary VLANs can be configured on this switch, and multiple community VLANs can be associated with each primary VLAN. (Note that private VLANs and normal VLANs can exist simultaneously within the same switch.)

To configure primary/secondary associated groups, follow these steps:

1. Use the Private VLAN Configuration page to designate one or more community VLANs, and the primary VLAN that will channel traffic outside of the VLAN groups.
2. Use the Private VLAN Association page to map a community VLAN to the primary VLAN.

3. Use the Private VLAN Port Configuration page to set the port type to promiscuous (i.e., having access to all ports in the primary VLAN), or host (i.e., having access restricted to community VLAN members, and channeling all other traffic through promiscuous ports). Then assign any promiscuous ports to a primary VLAN and any host ports a community VLAN.

DISPLAYING PRIVATE VLANS

The VLAN > Private VLAN > Information page to display information on the private VLANs configured on the switch, including primary and community VLANs, and their assigned interfaces.

CLI REFERENCES

- "show vlan private-vlan" on page 829

PARAMETERS

These parameters are displayed in the web interface:

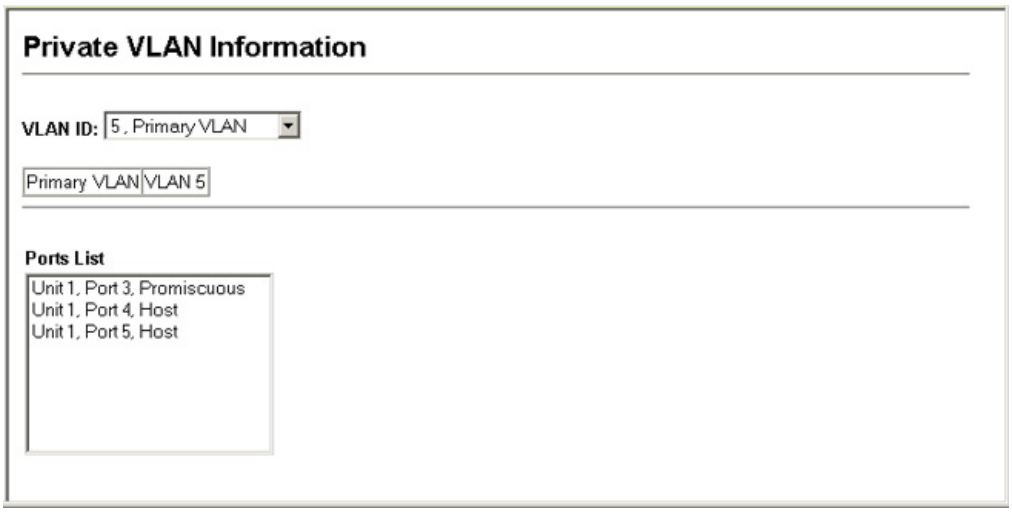
- **VLAN ID** – ID of configured VLAN (1-4094), and VLAN type.
- **Primary VLAN** – The VLAN with which the selected VLAN ID is associated. A primary VLAN displays its own ID, and a community VLAN displays the associated primary VLAN.
- **Ports List** – The list of ports (and assigned port type) in the selected private VLAN.

WEB INTERFACE

To display a list of private VLANs and the assigned members:

1. Click VLAN, Private VLAN, Information.
2. Select a primary or community VLAN from the drop-down list.

Figure 163: Showing Private VLANs



CREATING PRIVATE VLANS

Use the VLAN > Private VLAN > Configuration page to create primary or community VLANs.

CLI REFERENCES

- "private-vlan" on page 826

PARAMETERS

These parameters are displayed in the web interface:

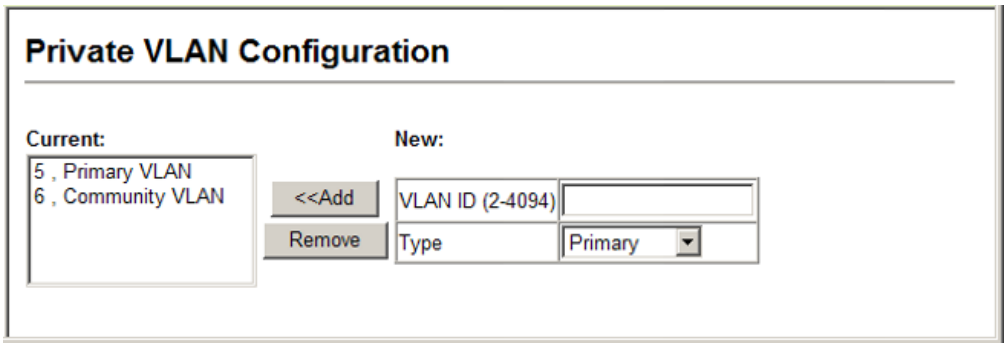
- **VLAN ID** – ID of configured VLAN (2-4094).
- **Type** – There are two types of private VLANs:
  - **Primary** – Conveys traffic between promiscuous ports, and to community ports within secondary (or community) VLANs.
  - **Community** - Conveys traffic between community ports, and to their promiscuous ports in the associated primary VLAN.

WEB INTERFACE

To configure private VLANs:

1. Click VLAN > Private VLAN > Configuration.
2. Enter the VLAN ID to assign to the private VLAN.
3. Select Primary or Community from the Type list
4. Click Apply.

Figure 164: Configuring Private VLANs



NOTE: All member ports must be removed from the VLAN before it can be deleted.

ASSOCIATING PRIVATE VLANS

Use the VLAN > Private VLAN > Association page to associate each community VLAN with a primary VLAN.

CLI REFERENCES

- "private vlan association" on page 827

PARAMETERS

These parameters are displayed in the web interface:

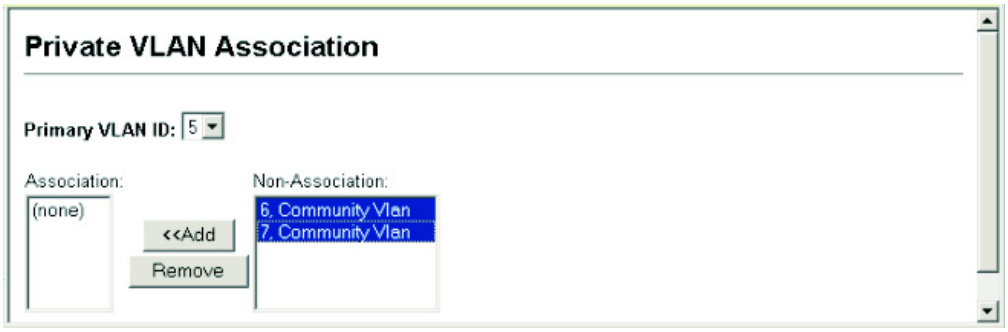
- **Primary VLAN** – ID of primary VLAN (2-4094).
- **Association** – Community VLANs associated with the selected primary VLAN.
- **Non-Association** – Community VLANs not associated with the selected VLAN.

WEB INTERFACE

To associate a community VLAN with a primary VLAN:

1. Click VLAN, Private VLAN, Association.
2. Select an entry from the Primary VLAN ID list.
3. Highlight one or more community VLANs in the Non-Association list box. Note that a community VLAN can only be associated with one primary VLAN.
4. Click Add.

Figure 165: Associating Private VLANs



DISPLAYING PRIVATE VLAN INTERFACE INFORMATION

Use the VLAN > Private VLAN > Port Information or Trunk Information page to display the interfaces associated with private VLANs.

CLI REFERENCES

- "show vlan private-vlan" on page 829

PARAMETERS

These parameters are displayed in the web interface:

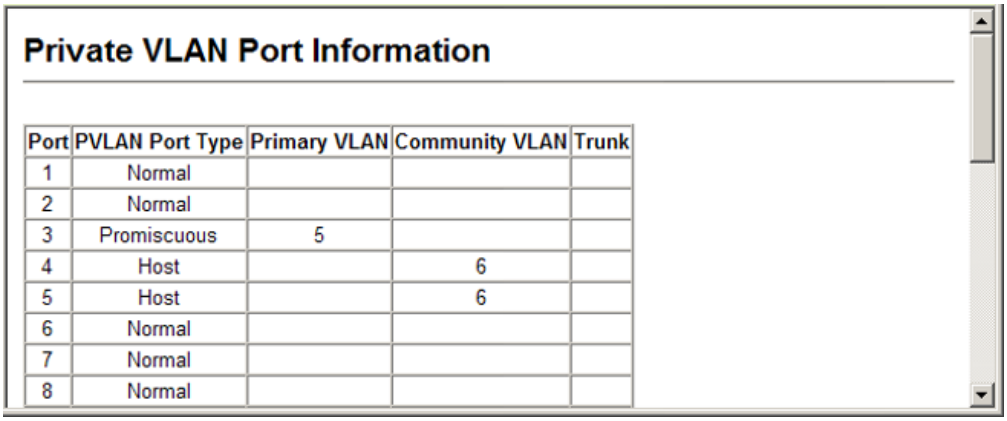
- **Port/Trunk** – The switch interface.
- **PVLAN Port Type** – Displays private VLAN port types.
  - **Normal** – The port is not configured in a private VLAN.
  - **Host** – The port is a community port and can only communicate with other ports in its own community VLAN, and with the designated promiscuous port(s). Or the port is an isolated port that can only communicate with the lone promiscuous port within its own isolated VLAN.
  - **Promiscuous** – A promiscuous port can communicate with all the interfaces within a private VLAN.
- **Primary VLAN** – Conveys traffic between promiscuous ports, and between promiscuous ports and community ports within the associated secondary VLANs.
- **Community VLAN** – A community VLAN conveys traffic between community ports, and from community ports to their designated promiscuous ports.
- **Trunk** – The trunk identifier. (Port Information only)

WEB INTERFACE

To display the interfaces associated with private VLANs:

1. Click VLAN, Private VLAN, Port Information.

Figure 166: Displaying Private VLAN Interfaces



CONFIGURING PRIVATE VLAN INTERFACES

Use the VLAN > Private VLAN > Port Configuration or Trunk Configuration page to set the private VLAN interface type, and assign the interfaces to a private VLAN.

CLI REFERENCES

- "switchport private-vlan mapping" on page 829
- "switchport private-vlan host-association" on page 828

PARAMETERS

These parameters are displayed in the web interface:

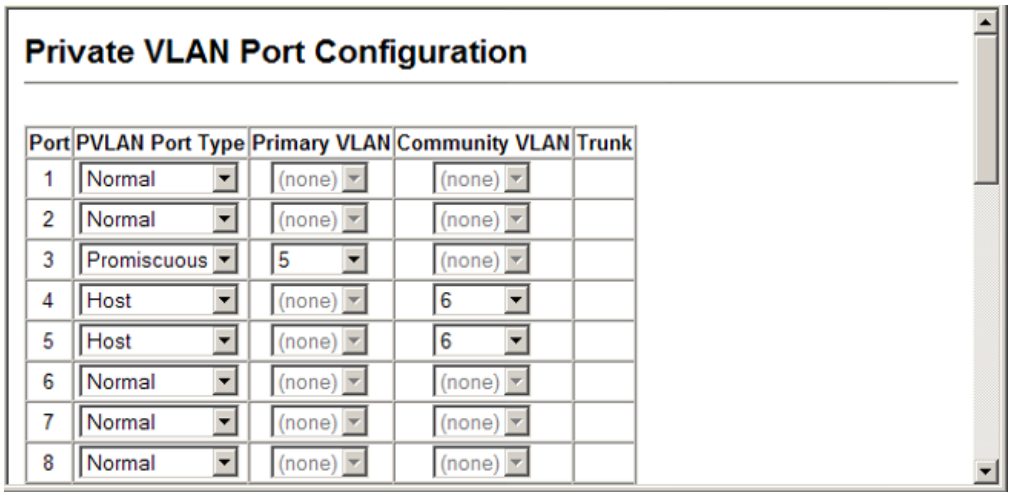
- **Port** – Port Identifier. (Range: 1-28/52)
- **Trunk** – Trunk Identifier. (Range: 1-8)
- **PVLAN Port Type** – Sets the private VLAN port types.
  - **Normal** – The port is not assigned to a private VLAN.
  - **Host** – The port is a community port. A community port can communicate with other ports in its own community VLAN and with designated promiscuous port(s).
  - **Promiscuous** – A promiscuous port can communicate with all interfaces within a private VLAN.
- **Primary VLAN** – Conveys traffic between promiscuous ports, and between promiscuous ports and community ports within the associated secondary VLANs. If Port Mode is "Promiscuous," then specify the associated primary VLAN.
- **Community VLAN** – A community VLAN conveys traffic between community ports, and from community ports to their designated promiscuous ports. Set Port Mode to "Host," and then specify the associated Community VLAN.
- **Trunk** – The trunk identifier. (Port Configuration only)

WEB INTERFACE

To configure a private VLAN port:

1. Click VLAN, Private VLAN, Port Configuration.
2. Set the Port Mode to Promiscuous or Host.
3. For an interface set the Promiscuous mode, select an entry from the Primary VLAN list.
4. For an interface set the Host mode, select an entry from the Community VLAN list.
5. Click Apply.

Figure 167: Configuring Interfaces for Private VLANs



PROTOCOL VLANS

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type being used by the inbound packets.

COMMAND USAGE

- To configure protocol-based VLANs, follow these steps:

  1. First configure VLAN groups for the protocols you want to use (page 804). Although not mandatory, we suggest configuring a separate VLAN for each major protocol running on your network. Do not add port members at this time.

  2. Create a protocol group for each of the protocols you want to assign to a VLAN using the Configuration page.

  3. Then map each protocol to the appropriate VLAN using the System Configuration page.

- When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

CONFIGURING PROTOCOL VLAN GROUPS

Use the VLAN > Protocol VLAN > Configuration page to create protocol groups.

CLI REFERENCES

- "protocol-vlan protocol-group (Configuring Groups)" on page 831

PARAMETERS

These parameters are displayed:

- **Protocol Group ID** – Protocol Group ID assigned to the Protocol VLAN Group. (Range: 1-2147483647)
- **Frame Type** – Choose either Ethernet, RFC 1042, or LLC Other as the frame type used by this protocol.
- **Protocol Type** – Specifies the protocol type to match. The available options are IP, ARP, RARP and PPPoE. If LLC Other is chosen for the Frame Type, the only available Protocol Type is IPX Raw.

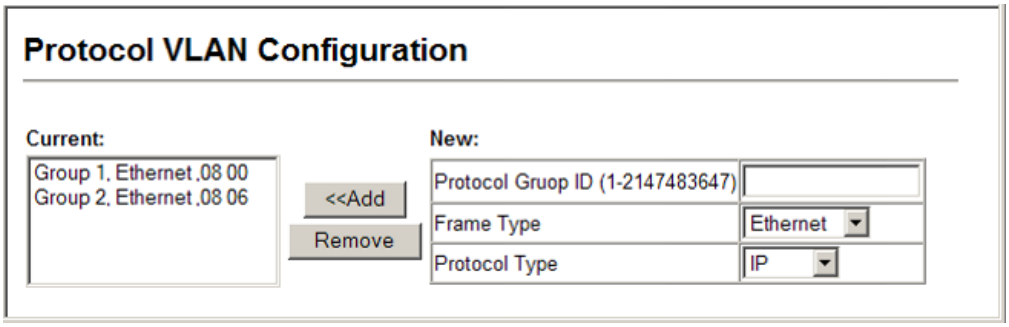
NOTE: Traffic which matches IP Protocol Ethernet Frames is mapped to the VLAN (VLAN 1) that has been configured with the switch's administrative IP. IP Protocol Ethernet traffic must not be mapped to another VLAN or you will lose administrative network connectivity to the switch. If lost in this manner, network access can be regained by removing the offending Protocol VLAN rule via the console. Alternately, the switch can be power-cycled, however all unsaved configuration changes will be lost.

WEB INTERFACE

To configure a protocol group:

1. Click VLAN, Protocol VLAN, Configuration.
2. Enter an identifier for the protocol group.
3. Select an entry from the Frame Type list.
4. Select an entry from the Protocol Type list.
5. Click Add.

Figure 168: Configuring Protocol VLANs



MAPPING PROTOCOL GROUPS TO VLANS

Use the VLAN > Protocol VLAN > System Configuration page to map a protocol group to each VLAN that will participate in the group.

CLI REFERENCES

- "protocol-vlan protocol-group (Configuring Interfaces)" on page 832

COMMAND USAGE

- When a frame enters a port that has been assigned to a protocol VLAN, it is processed in the following manner:
  - If the frame is tagged, it will be processed according to the standard rules applied to tagged frames.
  - If the frame is untagged and the protocol type matches, the frame is forwarded to the appropriate VLAN.
  - If the frame is untagged but the protocol type does not match, the frame is forwarded to the default VLAN for this interface.

PARAMETERS

These parameters are displayed:

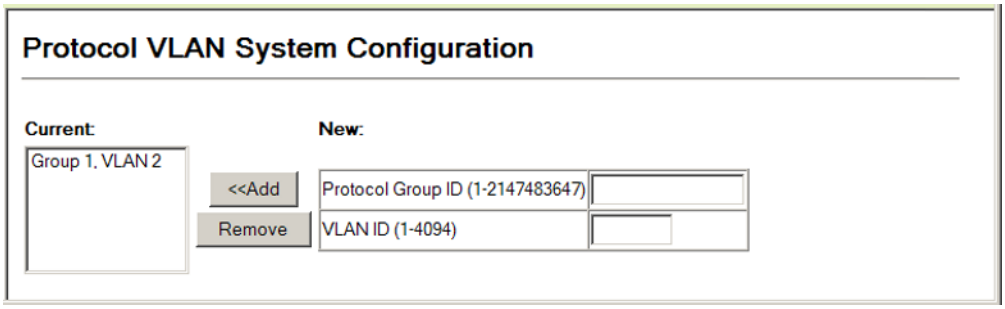
- **Protocol Group ID** – Protocol Group ID assigned to the Protocol VLAN Group. (Range: 1-2147483647)
- **VLAN ID** – VLAN to which matching protocol traffic is forwarded. (Range: 1-4094)

WEB INTERFACE

To map a protocol group to a VLAN for a port or trunk:

1. Click VLAN, Protocol VLA, System Configuration.
2. Enter the identifier for a protocol group.
3. Enter the corresponding VLAN to which the protocol traffic will be forwarded.
4. Click Add.

Figure 169: Assigning Protocols to VLANs



CONFIGURING VLAN MIRRORING

Use the VLAN > VLAN Mirror Configuration page to mirror traffic from one or more source VLANs to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source VLAN(s) in a completely unobtrusive manner.

CLI REFERENCES

- "Port Mirroring Commands" on page 713

COMMAND USAGE

- All active ports in a source VLAN are monitored for ingress traffic only.
- All VLAN mirror sessions must share the same target port, preferably one that is not a member of the source VLAN.
- When VLAN mirroring and port mirroring are both enabled, they must use the same target port.
- When VLAN mirroring and port mirroring are both enabled, the target port can receive a mirrored packet twice; once from the source mirror port and again from the source mirrored VLAN.
- The target port receives traffic from all monitored source VLANs and can become congested. Some mirror traffic may therefore be dropped from the target port.
- When mirroring VLAN traffic or packets based on a source MAC address (see "Configuring MAC Address Mirroring"), the target port cannot be set to the same target ports as that used for port mirroring (see "Configuring Port Mirroring").
- When traffic matches the rules for both port mirroring, and for mirroring of VLAN traffic or packets based on a MAC address, the matching packets will not be sent to target port specified for port mirroring.

PARAMETERS

These parameters are displayed:

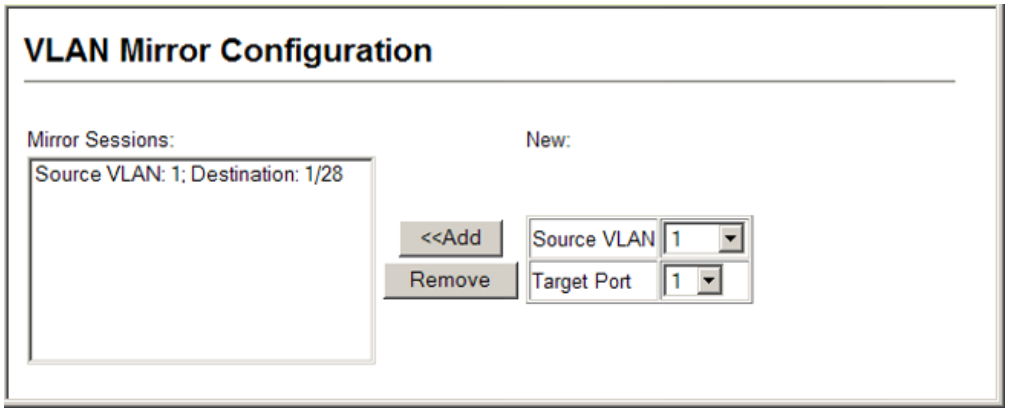
- **Source VLAN** – A VLAN whose traffic will be monitored. (Range: 1-4094)
- **Target Port** – The destination port that receives the mirrored traffic from the source VLAN. (Range: 1-28/52)

WEB INTERFACE

To configure VLAN mirroring:

1. Click VLAN, VLAN Mirror Configuration.
2. Select the source VLAN,
3. Select a target port that is not a member of the source VLAN.
4. Click Add.

Figure 170: Configuring VLAN Mirroring



CONFIGURING IP SUBNET VLANS

Use the VLAN > IP Subnet VLAN > Configuration page to configure IP subnet-based VLANs.

When using port-based classification, all untagged frames received by a port are classified as belonging to the VLAN whose VID (PVID) is associated with that port.

When IP subnet-based VLAN classification is enabled, the source address of untagged ingress frames are checked against the IP subnet-to-VLAN mapping table. If an entry is found for that subnet, these frames are assigned to the VLAN indicated in the entry. If no IP subnet is matched, the untagged frames are classified as belonging to the receiving port's VLAN ID (PVID).

CLI REFERENCES

- "Configuring IP Subnet VLANs" on page 834

COMMAND USAGE

- Each IP subnet can be mapped to only one VLAN ID. An IP subnet consists of an IP address and a mask.
- When an untagged frame is received by a port, the source IP address is checked against the IP subnet-to-VLAN mapping table, and if an entry is found, the corresponding VLAN ID is assigned to the frame. If no mapping is found, the PVID of the receiving port is assigned to the frame.
- The IP subnet cannot be a broadcast or multicast IP address.
- When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

PARAMETERS

These parameters are displayed:

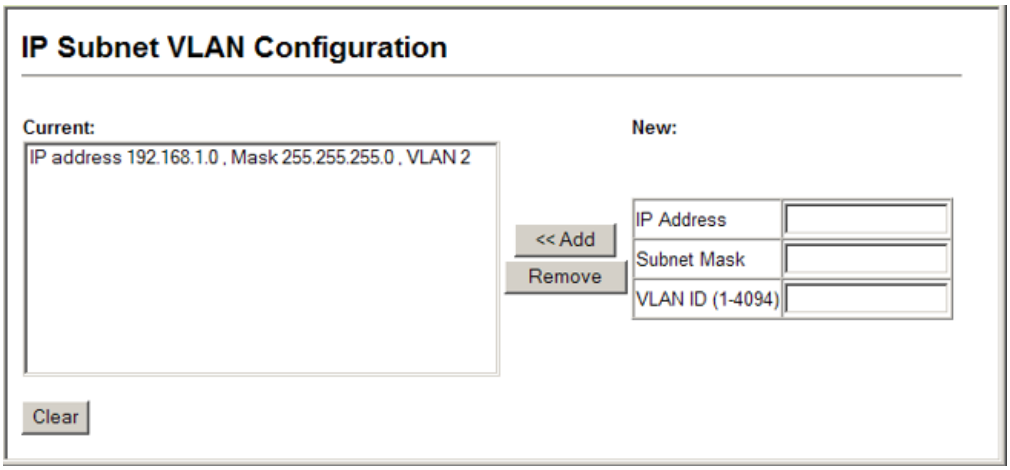
- **IP Address** – The IP address for a subnet. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.
- **Subnet Mask** – This mask identifies the host address bits of the IP subnet.
- **VLAN ID** – VLAN to which matching IP subnet traffic is forwarded. (Range: 1-4094)

WEB INTERFACE

To map an IP subnet to a VLAN:

1. Click VLAN, IP Subnet VLAN, Configuration.
2. Enter an address in the IP Address field.
3. Enter a mask in the Subnet Mask field.
4. Enter the identifier in the VLAN field. Note that the specified VLAN need not already be configured.
5. Click Add.

Figure 171: Configuring IP Subnet VLANs



CONFIGURING MAC-BASED VLANS

Use the VLAN > MAC-based VLAN > Configuration page to configure VLANs based on MAC addresses. The MAC-based VLAN feature assigns VLAN IDs to ingress untagged frames according to source MAC addresses.

When MAC-based VLAN classification is enabled, untagged frames received by a port are assigned to the VLAN which is mapped to the frame's source MAC address. When no MAC address is matched, untagged frames are assigned to the receiving port's native VLAN ID (PVID).

CLI REFERENCES

- "Configuring MAC Based VLANs" on page 836

COMMAND USAGE

- The MAC-to-VLAN mapping applies to all ports on the switch.
- Source MAC addresses can be mapped to only one VLAN ID.
- Configured MAC addresses cannot be broadcast or multicast addresses.

- When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

PARAMETERS

These parameters are displayed:

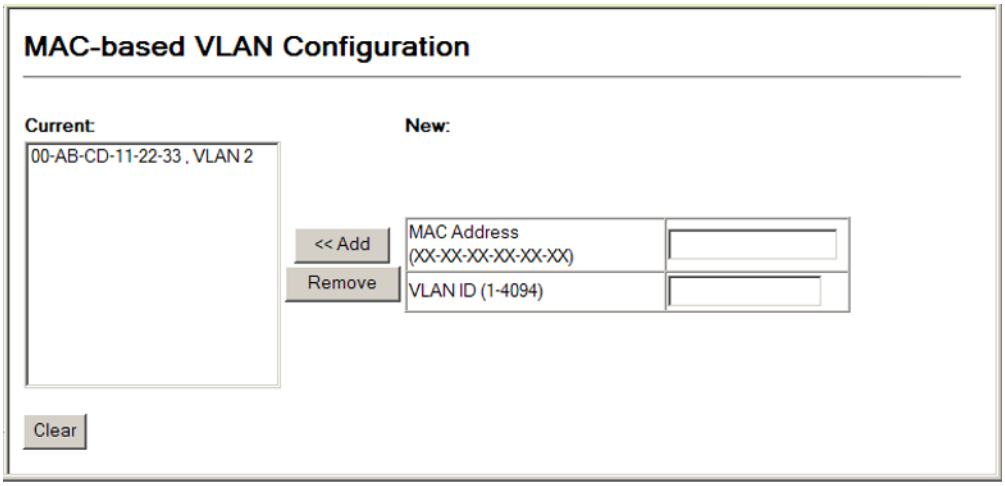
- **MAC Address** – A source MAC address which is to be mapped to a specific VLAN. The MAC address must be specified in the format xx-xx-xx-xx-xx-xx.
- **VLAN** – VLAN to which ingress traffic matching the specified source MAC address is forwarded. (Range: 1-4094)

WEB INTERFACE

To map a MAC address to a VLAN:

1. Click VLAN, MAC-based VLAN, Configuration.
2. Enter an address in the MAC Address field.
3. Enter an identifier in the VLAN field. Note that the specified VLAN need not already be configured.
4. Click Add.

Figure 172: Configuring MAC-Based VLANs



13 LINK LAYER DISCOVERY PROTOCOL

This chapter includes the following topics:

- LLDP Timing Attributes – Sets timing attributes for general functions.
- LLDP Interface Attributes – Specifies the advertised attributes for individual interfaces.
- LLDP Local Device Information – Displays information about the switch.
- LLDP Remote Port Information – Displays information about devices connected directly to the switch's ports.
- LLDP Remote Information Details – Displays detailed information about an LLDP-enabled device connected to a specific port on the switch.
- Device Statistics – Displays statistics for LLDP-capable devices attached to the switch, and for LLDP protocol messages transmitted or received on all local interfaces.
- Detailed Device Statistics – Displays detailed statistics for LLDP-capable devices attached to specific interfaces on the switch

OVERVIEW

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power, inventory, and device location details. LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

SETTING LLDP TIMING ATTRIBUTES

Use the LLDP > Configuration page to set attributes for general functions such as globally enabling LLDP on the switch, setting the message ageout time, and setting the frequency for broadcasting general advertisements or reports about changes in the LLDP MIB.

CLI REFERENCES

- "LLDP Commands" on page 905

PARAMETERS

These parameters are displayed:

- **LLDP** – Enables LLDP globally on the switch. (Default: Enabled)
- **Transmission Interval** – Configures the periodic transmit interval for LLDP advertisements. (Range: 5-32768 seconds; Default: 30 seconds)

  This attribute must comply with the following rule:
  (Transmission Interval * Hold Time Multiplier) ≤ 65536, and
  Transmission Interval >= (4 * Delay Interval)
- **Hold Time Multiplier** – Configures the time-to-live (TTL) value sent in LLDP advertisements as shown in the formula below. (Range: 2-10; Default: 4)

  The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner.

  TTL in seconds is based on the following rule:
  (Transmission Interval * Holdtime Multiplier) ≤ 65536.

  Therefore, the default TTL is 4*30 = 120 seconds.
- **Delay Interval** – Configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables. (Range: 1-8192 seconds; Default: 2 seconds)

  The transmit delay is used to prevent a series of successive LLDP transmissions during a short period of rapid changes in local LLDP MIB objects, and to increase the probability that multiple, rather than single changes, are reported in each transmission.

  This attribute must comply with the rule:
  (4 * Delay Interval) ≤ Transmission Interval
- **Reinitialization Delay** – Configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down.
  (Range: 1-10 seconds; Default: 2 seconds)

  When LLDP is re-initialized on a port, all information in the remote systems LLDP MIB associated with this port is deleted.

- **Notification Interval** – Configures the allowed interval for sending SNMP notifications about LLDP MIB changes. (Range: 5-3600 seconds; Default: 5 seconds)

  This parameter only applies to SNMP applications which use data stored in the LLDP MIB for network monitoring or management.

  Information about changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

- **MED Fast Start Count** – Configures the amount of LLDP MED Fast Start LLDPDUs to transmit during the activation process of the LLDP-MED Fast Start mechanism. (Range: 1-10 packets; Default: 4 packets)

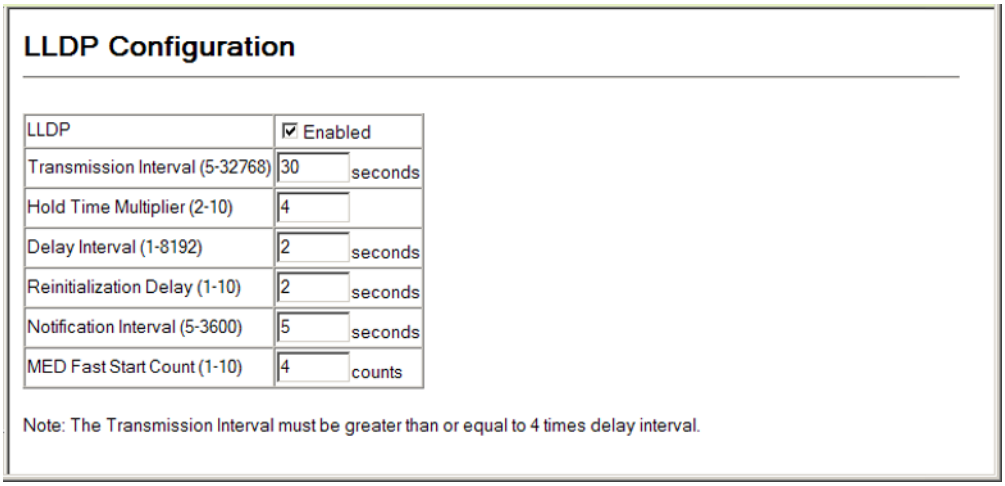
  The MED Fast Start Count parameter is part of the timer which ensures that the LLDP-MED Fast Start mechanism is active for the port. LLDP-MED Fast Start is critical to the timely startup of LLDP, and therefore integral to the rapid availability of Emergency Call Service.

WEB INTERFACE

To configure LLDP timing attributes:

1. Click LLDP, Configuration.
2. Enable LLDP, and modify any of the timing parameters as required.
3. Click Apply.

Figure 173: Configuring LLDP Timing Attributes



CONFIGURING LLDP INTERFACE ATTRIBUTES

Use the LLDP > Port Configuration or Trunk Configuration page to specify the message attributes for individual interfaces, including whether messages are transmitted, received, or both transmitted and received, whether SNMP notifications are sent, and the type of information advertised.

CLI REFERENCES

- "LLDP Commands" on page 905

PARAMETERS

These parameters are displayed:

- **Admin Status** – Enables LLDP message transmit and receive modes for LLDP Protocol Data Units. (Options: Tx only, Rx only, TxRx, Disabled; Default: TxRx)

- **SNMP Notification** – Enables the transmission of SNMP trap notifications about LLDP and LLDP-MED changes. (Default: Enabled)

  This option sends out SNMP trap notifications to designated target stations at the interval specified by the Notification Interval in the preceding section. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), the LLDP-MED MIB (ANSI/TIA-1057), or vendor-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs.

  For information on defining SNMP trap destinations, see "Specifying Trap Managers and Trap Types."

  Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

- **Admin Status** – Enables LLDP message transmit and receive modes for LLDP Protocol Data Units. (Options: Tx only, Rx only, TxRx, Disabled; Default: TxRx)

- **SNMP Notification** – Enables the transmission of SNMP trap notifications about LLDP and LLDP-MED changes. (Default: Enabled)

  This option sends out SNMP trap notifications to designated target stations at the interval specified by the Notification Interval in the preceding section. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), the LLDP-MED MIB (ANSI/TIA-1057), or vendor-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs.

  For information on defining SNMP trap destinations, see "Specifying Trap Managers and Trap Types."

Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

- **TLV Type** – Configures basic information included in the TLV field of advertised messages.
  - **Port Description** – The port description is taken from the ifDescr object in RFC 2863, which includes information about the manufacturer, the product name, and the version of the interface hardware/software.
  - **System Description** – The system description is taken from the sysDescr object in RFC 3418, which includes the full name and version identification of the system's hardware type, software operating system, and networking software.
  - **Management Address** – The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.

    The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address. The interface number and OID are included to assist SNMP applications in the performance of network discovery by indicating enterprise specific or other starting points for the search, such as the Interface or Entity MIB.

    Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV.

    Every management address TLV that reports an address that is accessible on a port and protocol VLAN through the particular port should be accompanied by a port and protocol VLAN TLV that indicates the VLAN identifier (VID) associated with the management address reported by this TLV.
  - **System Name** – The system name is taken from the sysName object in RFC 3418, which contains the system's administratively assigned name. To configure the system name, see "Displaying System Information".
  - **System Capabilities** – The system capabilities identifies the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.

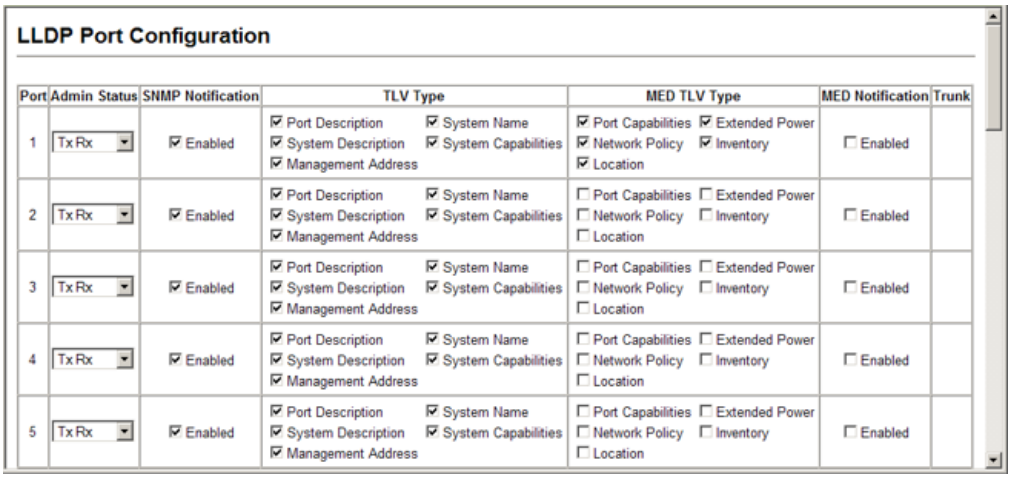
- **MED TLV Type** – Configures the information included in the MED TLV field of advertised messages.
  - **Port Capabilities** – This option advertises LLDP-MED TLV capabilities, allowing Media Endpoint and Connectivity Devices to efficiently discover which LLDP-MED related TLVs are supported on the switch.
  - **Network Policy** – This option advertises network policy configuration information, aiding in the discovery and diagnosis of VLAN configuration mismatches on a port. Improper network policy configurations frequently result in voice quality degradation or complete service disruption.
  - **Location** – This option advertises location identification details.
  - **Extended Power** – This option advertises extended Power-over-Ethernet capability details, such as power availability from the switch, and power state of the switch, including whether the switch is operating from primary or backup power (the Endpoint Device could use this information to decide to enter power conservation mode). Note that this device does not support PoE capabilities.
  - **Inventory** – This option advertises device details useful for inventory management, such as manufacturer, model, software version and other pertinent information.
- **MED Notification** – Enables the transmission of SNMP trap notifications about LLDP-MED changes. (Default: Enabled)
- **Trunk** – The trunk identifier. (Port Information only)

WEB INTERFACE

To configure LLDP interface attributes:

1. Click LLDP, Port Configuration.
2. Set the LLDP transmit/receive mode, specify whether or not to send SNMP trap messages, select the information to advertise in LLDP message, select the information to advertise in MED-TLV messages, and specify whether or not to send MED notifications.
3. Click Apply.

Figure 174: Configuring LLDP Interface Attributes



DISPLAYING LLDP LOCAL DEVICE INFORMATION

Use the LLDP > Local Information page to display information about the switch, such as its MAC address, chassis ID, management IP address, and port information.

CLI REFERENCES

- "show lldp info local-device" on page 923

PARAMETERS

These parameters are displayed:

Global Settings

- **Chassis Type** – Identifies the chassis containing the IEEE 802 LAN entity associated with the transmitting LLDP agent. There are several ways in which a chassis may be identified and a chassis ID subtype is used to indicate the type of component being referenced by the chassis ID field.

Table 25: Chassis ID Subtype

ID Basis	Reference
Chassis component	EntPhysicalAlias when entPhysClass has a value of 'chassis(3)' (IETF RFC 2737)
Interface alias	IfAlias (IETF RFC 2863)
Port component	EntPhysicalAlias when entPhysicalClass has a value 'port(10)' or 'backplane(4)' (IETF RFC 2737)
MAC address	MAC address (IEEE Std 802-2001)
Network address	networkAddress
Interface name	ifName (IETF RFC 2863)
Locally assigned	locally assigned

- **Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.
- **System Name** – A string that indicates the system's administratively assigned name (see "Displaying System Information").
- **System Description** – A textual description of the network entity. This field is also displayed by the **show system** command.
- **System Capabilities Supported** – The capabilities that define the primary function(s) of the system.

Table 26: System Capabilities

ID Basis	Reference
Other	—
Repeater	IETF RFC 2108
Bridge	IETF RFC 2674
WLAN Access Point	IEEE 802.11 MIB
Router	IETF RFC 1812
Telephone	IETF RFC 2011
DOCSIS cable device	IETF RFC 2669 and IETF RFC 2670
End Station Only	IETF RFC 2011

- **System Capabilities Enabled** – The primary function(s) of the system which are currently enabled. Refer to the preceding table.
- **Management Address** – The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.

Interface Settings

The attributes listed below apply to both port and trunk interface types. When a trunk is listed, the descriptions apply to the first port of the trunk.

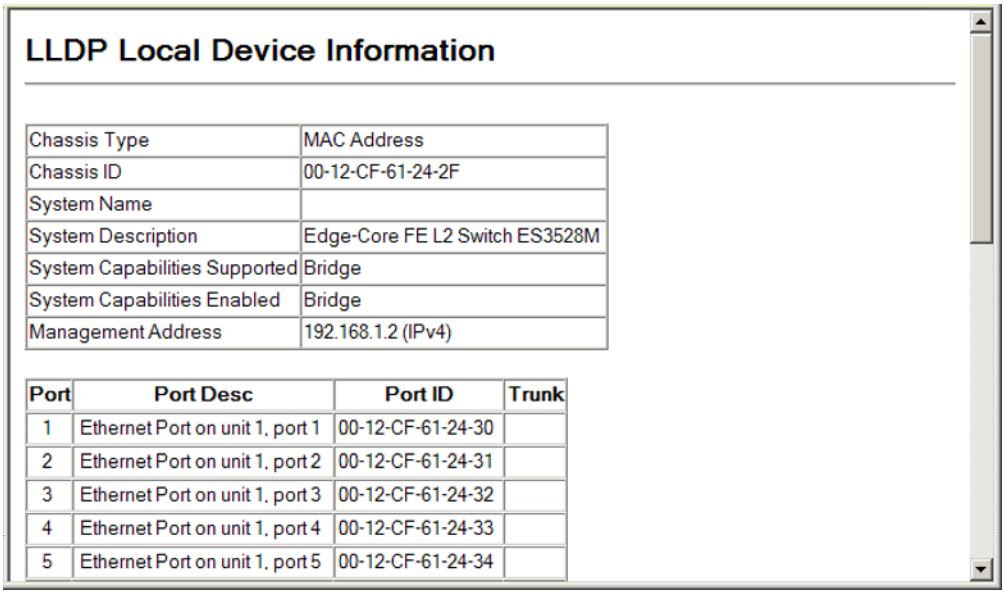
- **Port/Trunk Description** – A string that indicates the port or trunk description. If RFC 2863 is implemented, the ifDescr object should be used for this field.
- **Port/Trunk ID** – A string that contains the specific identifier for the port or trunk from which this LLDPDU was transmitted.

WEB INTERFACE

To display LLDP information for the local device:

1. Click LLDP, Local Information.

Figure 175: Displaying Local Device Information for LLDP



LLDP Local Device Information

Chassis Type	MAC Address
Chassis ID	00-12-CF-61-24-2F
System Name	
System Description	Edge-Core FE L2 Switch ES3528M
System Capabilities Supported	Bridge
System Capabilities Enabled	Bridge
Management Address	192.168.1.2 (IPv4)

Port	Port Desc	Port ID	Trunk
1	Ethernet Port on unit 1, port 1	00-12-CF-61-24-30	
2	Ethernet Port on unit 1, port 2	00-12-CF-61-24-31	
3	Ethernet Port on unit 1, port 3	00-12-CF-61-24-32	
4	Ethernet Port on unit 1, port 4	00-12-CF-61-24-33	
5	Ethernet Port on unit 1, port 5	00-12-CF-61-24-34	

DISPLAYING LLDP REMOTE PORT INFORMATION

Use the LLDP > Remote Port Information page to display information about devices connected directly to the switch's ports which are advertising information through LLDP.

CLI REFERENCES

- "show lldp info remote-device" on page 924

PARAMETERS

These parameters are displayed:

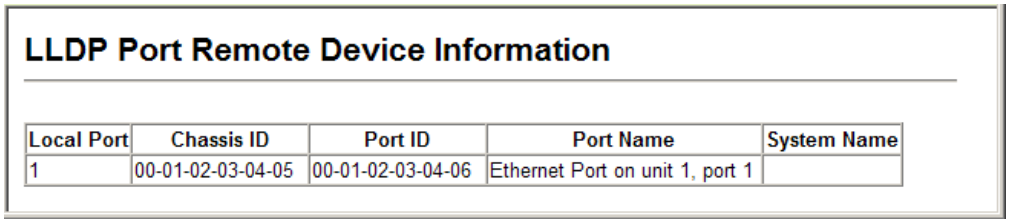
- **Local Port** – The local port to which a remote LLDP-capable device is attached.
- **Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.
- **Port ID** – A string that contains the specific identifier for the port from which this LLDPDU was transmitted.
- **Port Name** – A string that indicates the port's description. If RFC 2863 is implemented, the ifDescr object should be used for this field.
- **System Name** – A string that indicates the system's administratively assigned name.

WEB INTERFACE

To display LLDP information for a remote port:

1. Click LLDP, Remote Port Information.

Figure 176: Displaying Remote Device Information for LLDP



DISPLAYING LLDP REMOTE INFORMATION DETAILS

Use the LLDP > Remote Information Details page to display detailed information about an LLDP-enabled device connected to a specific port on the local switch.

- "show lldp info remote-device" on page 924

PARAMETERS

These parameters are displayed:

Port Details

- **Local Port** – The local port to which a remote LLDP-capable device is attached.
- **Chassis Type** – Identifies the chassis containing the IEEE 802 LAN entity associated with the transmitting LLDP agent. There are several ways in which a chassis may be identified and a chassis ID subtype is used to indicate the type of component being referenced by the chassis ID field. (See Table 25, "Chassis ID Subtype," on page 367.)
- **Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.
- **Port Type** – Indicates the basis for the identifier that is listed in the Port ID field.

Table 27: Port ID Subtype

ID Basis	Reference
Interface alias	IfAlias (IETF RFC 2863)
Chassis component	EntPhysicalAlias when entPhysClass has a value of 'chassis(3)' (IETF RFC 2737)
Port component	EntPhysicalAlias when entPhysicalClass has a value 'port(10)' or 'backplane(4)' (IETF RFC 2737)

Table 27: Port ID Subtype (Continued)

ID Basis	Reference
MAC address	MAC address (IEEE Std 802-2001)
Network address	networkAddress
Interface name	ifName (IETF RFC 2863)
Agent circuit ID	agent circuit ID (IETF RFC 3046)
Locally assigned	locally assigned

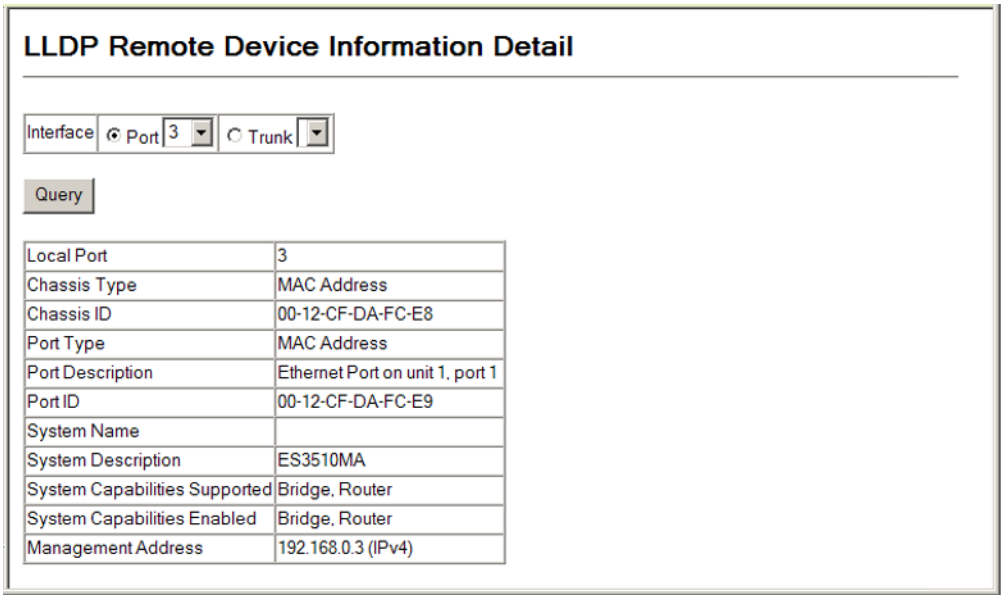
- **Port Description** – A string that indicates the port's description. If RFC 2863 is implemented, the ifDescr object should be used for this field.
- **Port ID** – A string that contains the specific identifier for the port from which this LLDPDU was transmitted.
- **System Name** – A string that indicates the system's assigned name.
- **System Description** – A textual description of the network entity.
- **System Capabilities Supported** – The capabilities that define the primary function(s) of the system. (See Table 26, "System Capabilities," on page 368.)
- **System Capabilities Enabled** – The primary function(s) of the system which are currently enabled. (See Table 26, "System Capabilities," on page 368.)
- **Management Address** – The management address for this device. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.

WEB INTERFACE

To display detailed LLDP information for a remote port:

1. Click LLDP, Remote Information Details.
2. Select a port or trunk from the scroll-down list.
3. Click Query.

Figure 177: Displaying Remote Device Information Details for LLDP



DISPLAYING DEVICE STATISTICS

Use the LLDP > Device Statistics page to display statistics for LLDP-capable devices attached to the switch, and for LLDP protocol messages transmitted or received on all local interfaces.

CLI REFERENCES

- "show lldp info statistics" on page 925

PARAMETERS

These parameters are displayed:

General Statistics on Remote Devices

- **Neighbor Entries List Last Updated** – The time the LLDP neighbor entry list was last updated.
- **New Neighbor Entries Count** – The number of LLDP neighbors for which the remote TTL has not yet expired.
- **Neighbor Entries Deleted Count** – The number of LLDP neighbors which have been removed from the LLDP remote systems MIB for any reason.
- **Neighbor Entries Dropped Count** – The number of times which the remote database on this switch dropped an LLDPDU because of insufficient resources.
- **Neighbor Entries Age-out Count** – The number of times that a neighbor's information has been deleted from the LLDP remote systems MIB because the remote TTL timer has expired.

Port/Trunk

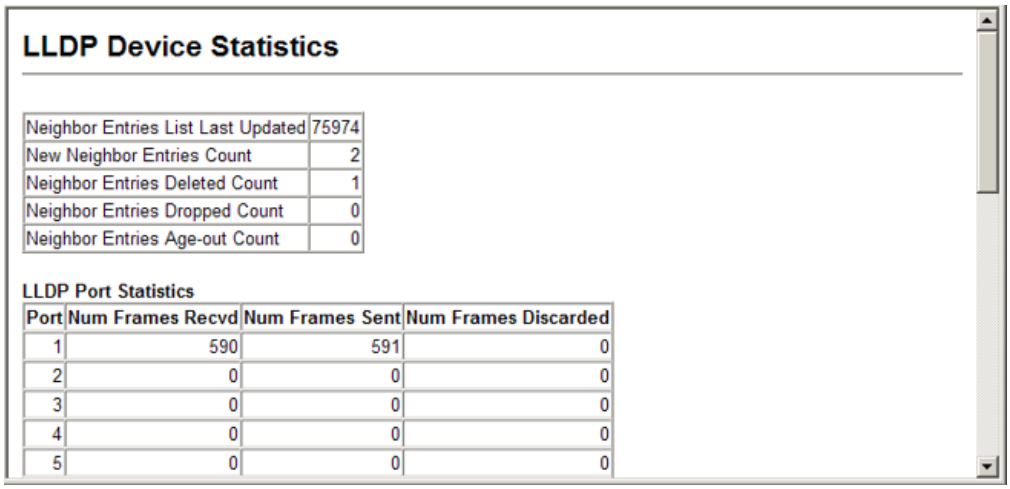
- **Num Frames Received** – Number of LLDP PDUs received.
- **Num Frames Sent** – Number of LLDP PDUs transmitted.
- **Num Frames Discarded** – Number of frames discarded because they did not conform to the general validation rules as well as any specific usage rules defined for the particular TLV.

WEB INTERFACE

To display statistics for LLDP-capable devices attached to the switch:

1. Click LLDP, Device Statistics.

Figure 178: Displaying LLDP Device Statistics



DISPLAYING DETAILED DEVICE STATISTICS

Use the LLDP > Device Statistics Details page to display detailed statistics for LLDP-capable devices attached to specific interfaces on the switch.

CLI REFERENCES

- "show lldp info statistics" on page 925

PARAMETERS

These parameters are displayed:

- **Frames Discarded** – Number of frames discarded because they did not conform to the general validation rules as well as any specific usage rules defined for the particular TLV.
- **Frames Invalid** – A count of all LLDPDUs received with one or more detectable errors.
- **Frames Received** – Number of LLDP PDUs received.

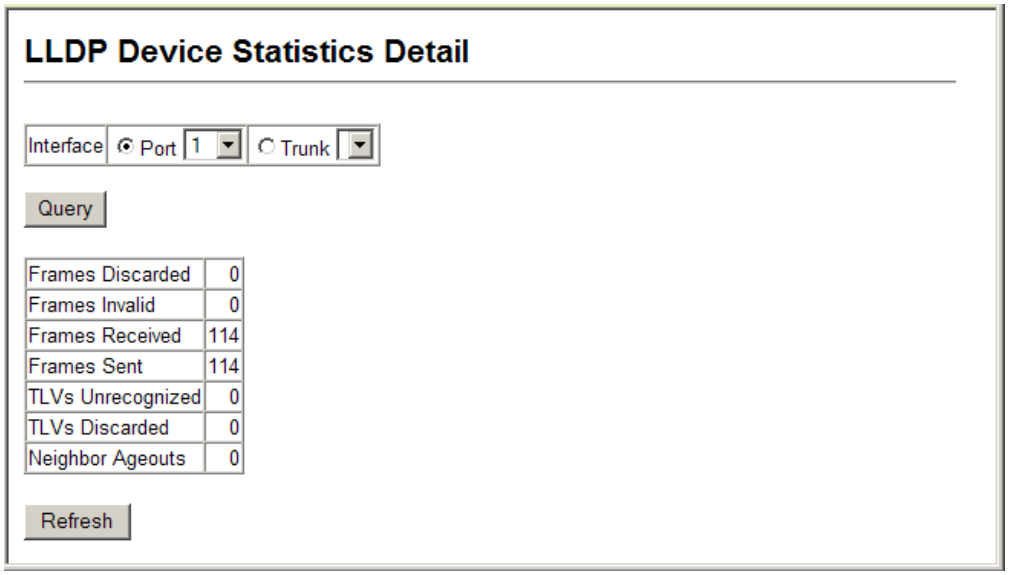
- **Frames Sent** – Number of LLDP PDUs transmitted.
- **TLVs Unrecognized** – A count of all TLVs not recognized by the receiving LLDP local agent.
- **TLVs Discarded** – A count of all LLDPDUs received and then discarded due to insufficient memory space, missing or out-of-sequence attributes, or any other reason.
- **Neighbor Ageouts** – A count of the times that a neighbor's information has been deleted from the LLDP remote systems MIB because the remote TTL timer has expired.

WEB INTERFACE

To display detailed statistics for LLDP-capable devices attached to the switch:

1. Click LLDP, Device Statistics Details.

Figure 179: Displaying LLDP Detailed Device Statistics



14 CLASS OF SERVICE

Class of Service (CoS) allows you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with four priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, and configure the mapping of frame priority tags to the switch's priority queues.

This chapter describes the following basic topics:

- Layer 2 Queue Settings – Configures each queue, including the default priority, queue mode, queue weight, and mapping of packets to queues based on CoS tags.
- Layer 3/4 Priority Settings – Selects the method by which inbound packets are processed (DSCP or CoS), and sets the per-hop behavior and drop precedence for internal processing.

LAYER 2 QUEUE SETTINGS

This section describes how to configure the default priority for untagged frames, set the queue mode, and map class of service tags to queues.

SETTING THE DEFAULT PRIORITY FOR INTERFACES

Use the Priority > Default Port Priority or Default Trunk Priority page to specify the default port priority for each interface on the switch. All untagged packets entering the switch are tagged with the specified default port priority, and then sorted into the appropriate priority queue at the output port.

CLI REFERENCES

- "switchport priority default" on page 848

COMMAND USAGE

- This switch provides four priority queues for each port. It uses Weighted Round Robin to prevent head-of-queue blockage.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.

- If the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.

PARAMETERS

These parameters are displayed:

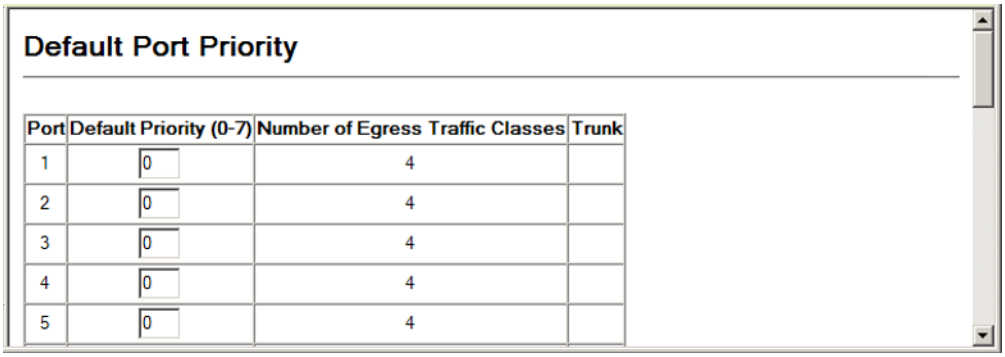
- **Default Priority** – The priority that is assigned to untagged frames received on the specified interface. (Range: 0-7; Default: 0)
- **Number of Egress Traffic Classes** – The number of queue buffers provided for each port.

WEB INTERFACE

To configure the queue mode:

1. Click Priority, Default Port Priority.
2. Modify the default priority for any interface.
3. Click Apply.

Figure 180: Setting the Default Port Priority



MAPPING COS VALUES TO EGRESS QUEUES

Use the Priority > Traffic Classes page to specify which of the hardware output queues to use for Class of Service (CoS) priority tagged traffic.

The switch processes priority tagged traffic by using four priority queues for each port, with service schedules based on strict priority or Weighted Round-Robin (WRR). Up to eight traffic priorities are defined in the IEEE 802.1p standard. Default priority levels are assigned according to recommendations in IEEE 802.1p as shown in the following table.

Table 28: IEEE 802.1p Egress Queue Priority Mapping

Priority	0	1	2	3	4	5	6	7
Queue	1	0	0	1	2	2	3	3

The priority levels recommended in the IEEE 802.1p standard for various network applications are shown in Table 29. However, priority levels can be

mapped to the switch's output queues in any way that benefits application traffic for the network.

Table 29: CoS Priority Levels

Priority Level	Traffic Type
1	Background
2	(Spare)
0 (default)	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

CLI REFERENCES

- "queue cos-map" on page 847

COMMAND USAGE

- Egress packets are placed into the hardware queues according to the mapping defined by this command.
- The specified mapping applies to all interfaces.

PARAMETERS

These parameters are displayed:

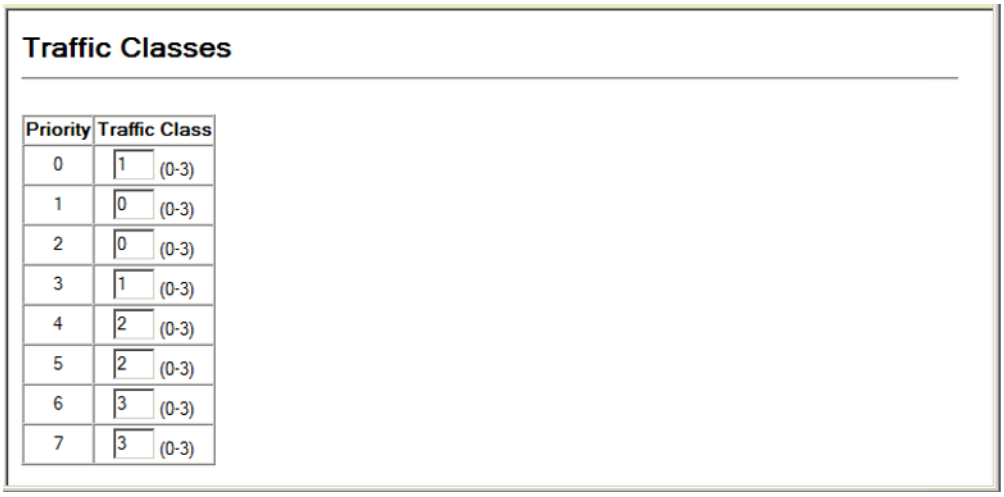
- **Priority** – CoS value. (Range: 0-7, where 7 is the highest priority)
- **Traffic Class** – Output queue buffer. (Range: 0-3, where 3 is the highest CoS priority queue)

WEB INTERFACE

To specify which of the output queues to use for CoS priority tagged traffic:

1. Click Priority, Traffic Classes.
2. Assign priorities to the traffic classes (i.e., output queues).
3. Click Apply.

Figure 181: Mapping CoS Values to Egress Queues



SELECTING THE QUEUE MODE

Use the Priority > Queue Mode page to set the queue mode for the egress queues on all interfaces. The switch can be set to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before the lower priority queues are serviced, or to use Weighted Round-Robin (WRR) queuing that specifies a scheduling weight for each queue.

CLI REFERENCES

- "queue mode" on page 846
- "show queue mode" on page 850

COMMAND USAGE

- Strict priority requires all traffic in a higher priority queue to be processed before lower priority queues are serviced.
- WRR uses a relative weighting for each queue which determines the amount of packets the switch transmits every time it services each queue before moving on to the next queue. Thus, a queue weighted 8 will be allowed to transmit up to 8 packets, after which the next lower priority queue will be serviced according to it's weighting. This prevents the head-of-line blocking that can occur with strict priority queuing.
- The specified queue mode applies to all interfaces.

PARAMETERS

These parameters are displayed:

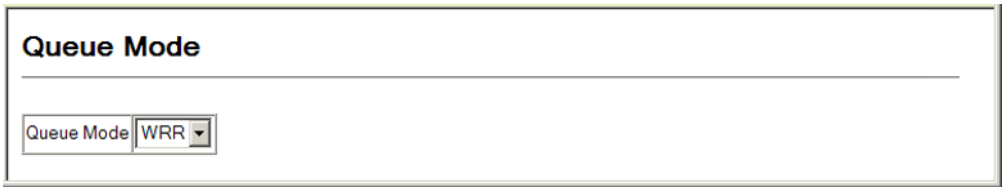
- **WRR** (WRR) – Shares bandwidth at the egress ports by using scheduling weights, servicing each queue in a round-robin fashion.
- **Strict** – Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues. This ensures that the highest priority packets are always serviced first, ahead of all other traffic.

WEB INTERFACE

To configure the queue mode:

1. Click Priority, Queue Mode.
2. Set the queue mode.
3. Click Apply.

Figure 182: Setting the Queue Mode



DISPLAYING THE SERVICE WEIGHT FOR TRAFFIC CLASSES

Use the Priority > Queue Scheduling page to display the weighted round-robin (WRR) bandwidth allocation for the four priority queues.

This switch uses the Weighted Round Robin (WRR) algorithm to determine the frequency at which it services each priority queue. As described in "Mapping CoS Values to Egress Queues," the traffic classes are mapped to one of the four egress queues provided for each port. This weight sets the limit for the number of packets the switch will transmit each time the queue is serviced, and subsequently affects the response time for software applications assigned a specific priority value.

NOTE: This switch does not allow the queue service weights to be set. The weights are fixed as 1, 2, 4, 8, for queues 0 through 3 respectively.

CLI REFERENCES

- "show queue bandwidth" on page 849

PARAMETERS

These parameters are displayed:

- **WRR Setting Table** – Displays a list of weights for each traffic class (i.e., queue).
- **Weight Value** – Displays the weight for each traffic class.

WEB INTERFACE

To display the WRR bandwidth allocation for the priority queues:

1. Click Priority, Queue Scheduling.

Figure 183: Showing the Queue Bandwidth Allocation

LAYER 3/4 PRIORITY SETTINGS

Mapping Layer 3/4 Priorities to CoS Values

The switch supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic priorities can be specified in the IP header of a frame, using the priority bits in the Type of Service (ToS) octet, or the number of the TCP/UDP port. If priority bits are used, the ToS octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

Because different priority information may be contained in the traffic, this switch maps priority values to the output queues in the following manner – The precedence for priority mapping is DSCP Priority and then Default Port Priority.

NOTE: The default settings used for mapping priority values from ingress traffic to internal DSCP values are used to determine the hardware queues used for egress traffic, not to replace the priority values. These defaults are designed to optimize priority services for the majority of network applications. It should not be necessary to modify any of the default settings, unless a queuing problem occurs with a particular application.

ENABLING IP DSCP PRIORITY

Use the Priority > IP DSCP Priority Status page to enable or disable the IP DSCP priority (i.e., Differentiated Services Code Point mapping).

CLI REFERENCES

- "map ip dscp (Global Configuration)" on page 850

PARAMETERS

These parameters are displayed:

- **IP DSCP Priority Status** – The following options are:

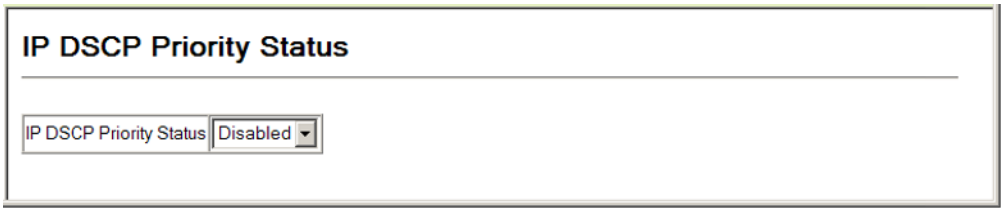
- **Disabled** – Disables the priority service. (Default Setting: Disabled)
- **IP DSCP** – Maps layer 3/4 priorities using Differentiated Services Code Point Mapping.

WEB INTERFACE

To enable or disable IP DSCP priority:

1. Click Priority, IP DSCP Priority Status.
2. Select Disabled or IP DSCP from the drop down menu.
3. Click Apply.

Figure 184: Setting IP DSCP Priority Status



MAPPING DSCP PRIORITY

Use the Priority > IP DSCP Priority page to set the IP DSCP (i.e., Differentiated Services Code Point priority) to CoS priority map.

CLI REFERENCES

◆ "show map ip dscp" on page 852

COMMAND USAGE

The DSCP is six bits wide, allowing coding for up to 64 different forwarding behaviors. The DSCP retains backward compatibility with the three precedence bits so that non-DSCP compliant devices will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP default mapping is defined in the following table. Note that all the DSCP values that are not specified are mapped to CoS value 0.

Table 30: Mapping DSCP Priority Values

IP DSCP Value	CoS Value
1	Background
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5

Table 30: Mapping DSCP Priority Values (Continued)

IP DSCP Value	CoS Value
48	6
46, 56	7

PARAMETERS

These parameters are displayed:

- **DSCP Priority Table –** Shows the DSCP Priority to CoS map.
- **Class of Service Value –** Maps a CoS value to the selected DSCP Priority value. Note that "0" represents low priority and "7" represent high priority.

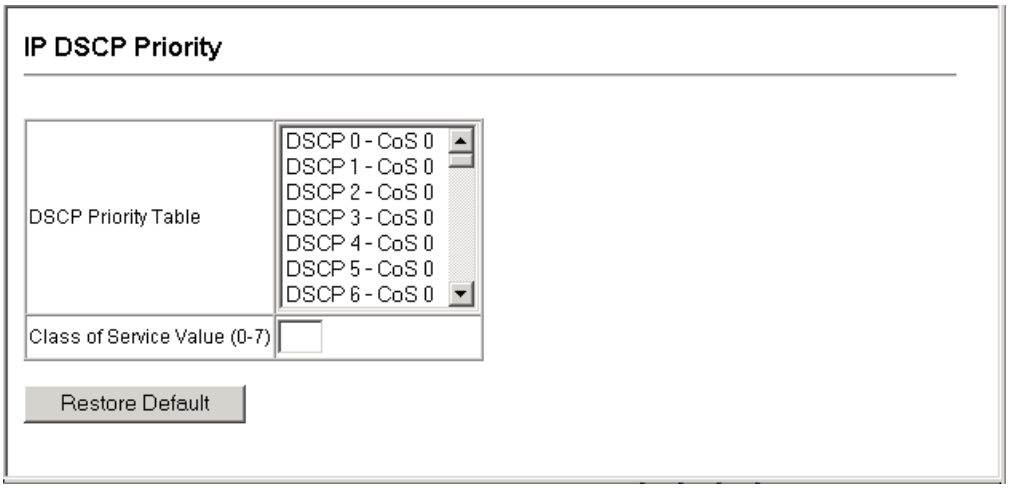
NOTE: IP DSCP settings apply to all interfaces.

WEB INTERFACE

To set the IP DSCP to CoS priority map:

1. Click Priority, IP DSCP Priority.
2. Select an entry from the DSCP table, and enter a value in the Class of Service Value field.
3. Click Apply.

Figure 185: Mapping IP DSCP Priority Values



15 QUALITY OF SERVICE

This chapter describes the following tasks required to apply QoS policies:

Class Map – Creates a map which identifies a specific class of traffic.

Policy Map – Sets the boundary parameters used for monitoring inbound traffic, and the action to take for conforming and non-conforming traffic.

Binding to a Port – Applies a policy map to an ingress port.

OVERVIEW

The commands described in this section are used to configure Quality of Service (QoS) classification criteria and service policies. Differentiated Services (DiffServ) provides policy-based management mechanisms used for prioritizing network resources to meet the requirements of specific traffic types on a per hop basis. Each packet is classified upon entry into the network based on access lists, IP Precedence, DSCP values, or VLAN lists. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet. Based on configured network policies, different kinds of traffic can be marked for different kinds of forwarding.

All switches or routers that access the Internet rely on class information to provide the same forwarding treatment to packets in the same class. Class information can be assigned by end hosts, or switches or routers along the path. Priority can then be assigned based on a general policy, or a detailed examination of the packet. However, note that detailed examination of packets should take place close to the network edge so that core switches and routers are not overloaded.

Switches and routers along the path can use class information to prioritize the resources allocated to different traffic classes. The manner in which an individual device handles traffic in the DiffServ architecture is called per-hop behavior. All devices along a path should be configured in a consistent manner to construct a consistent end-to-end QoS solution.

NOTE: You can configure up to 1024 rules per class map. You can also include multiple classes in a policy map.

NOTE: You should create a class map before creating a policy map. Otherwise, you will not be able to select a class map from the policy rule settings screen (see page 387).

COMMAND USAGE

To create a service policy for a specific category or ingress traffic, follow these steps:

1. Use the Class Map (Add Class) page to designate a class name for a specific category of traffic.
2. Use the Class Map (Edit Rules) page to edit the rules for each class to specify a type of traffic based on an access list, a DSCP or IP Precedence value, or a VLAN.
3. Use the Policy Map (Add Policy) page to designate a policy name for a specific manner in which ingress traffic will be handled.
4. Use the Policy Map (Edit Classes) page to add one or more classes to the policy map. Assign policy rules to each class by "setting" the QoS value to be assigned to the matching traffic class. The policy rule can also be configured to monitor the maximum throughput and burst rate. Then specify the action to take for conforming traffic, or the action to take for a policy violation.
5. Use the Service Policy page to assign a policy map to a specific interface.

CONFIGURING A CLASS MAP

Use the QoS > DiffServ > Class Map page to configure a class map. A class map is used for matching packets to a specified class.

CLI REFERENCES

- "Quality of Service Commands" on page 853

COMMAND USAGE

- To configure a Class Map, follow these steps:
  - Open the Class Map page, and click Add Class.
  - When the Class Configuration page opens, fill in the "Class Name" field, and click Add.
  - When the Match Class Settings page opens, specify type of traffic for this class based on an access list, a DSCP or IP Precedence value, or a VLAN, and click the Add button next to the field for the selected traffic criteria. You can specify up to 1024 items to match when assigning ingress traffic to a class map.
- The class map is used with a policy map (page 387) to create a service policy (page 391) for a specific interface that defines packet classification, service tagging, and bandwidth policing. Note that one or more class maps can be assigned to a policy map.

- Up to 1024 class statements can be configured for the system.

PARAMETERS

These parameters are displayed:

Class Map

- **Modify Name and Description** – Configures the name and a brief description of a class map. (Range: 1-16 characters for the name; 1-64 characters for the description)
- **Edit Rules** – Opens the "Match Class Settings" page for the selected class entry. Modify the criteria used to classify ingress traffic on this page.
- **Add Class** – Opens the "Class Configuration" page. Enter a class name and description on this page, and click Add to open the "Match Class Settings" page. Enter the criteria used to classify ingress traffic on this page.
- **Remove Class** – Removes the selected class.

Class Configuration (Add Class)

- **Class Name** – Name of the class map. (Range: 1-16 characters)
- **Type** – Only one match command is permitted per class map, so the match-any field refers to the criteria specified by the lone match command.
- **Description** – A brief description of a class map. (Range: 1-64 characters)
- **Add** – Adds the specified class.
- **Back** – Returns to previous page with making any changes.

Match Class Settings (Edit Rules)

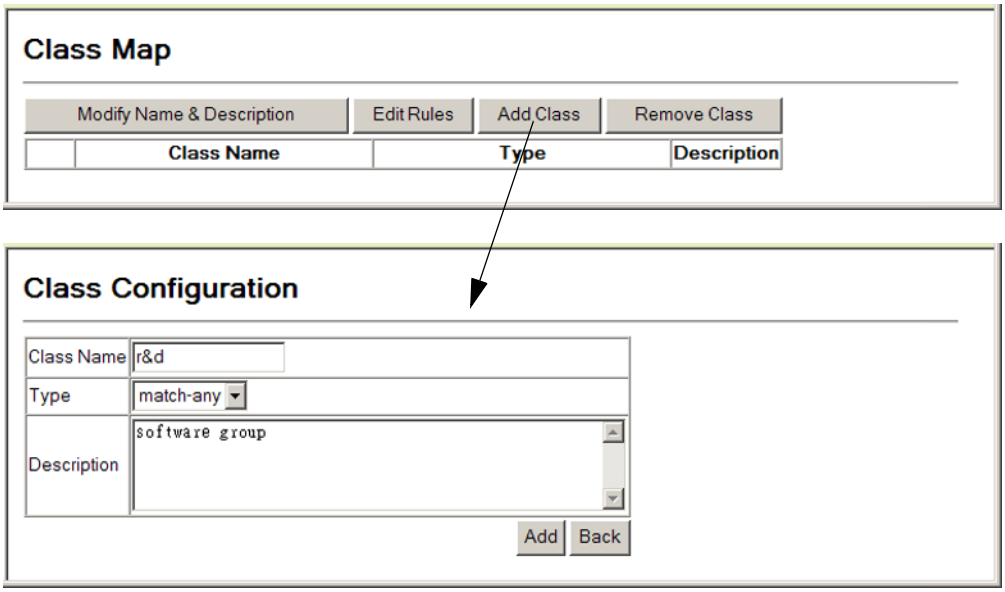
- **Class Name** – Name of the class map.
- **ACL List** – Name of an access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs.
- **IP DSCP** – A DSCP value. (Range: 0-63)
- **IP Precedence** – An IP Precedence value. (Range: 0-7)
- **VLAN ID** – A VLAN. (Range:1-4094)
- **Add** – Adds specified criteria to the class. Up to 16 items are permitted per class.
- **Remove** – Deletes the selected criteria from the class.

WEB INTERFACE

To create a class map:

1. Click QoS, DiffServ, Class Map.
2. Click Add Class.
3. Enter a class name and a description.
4. Click Add.

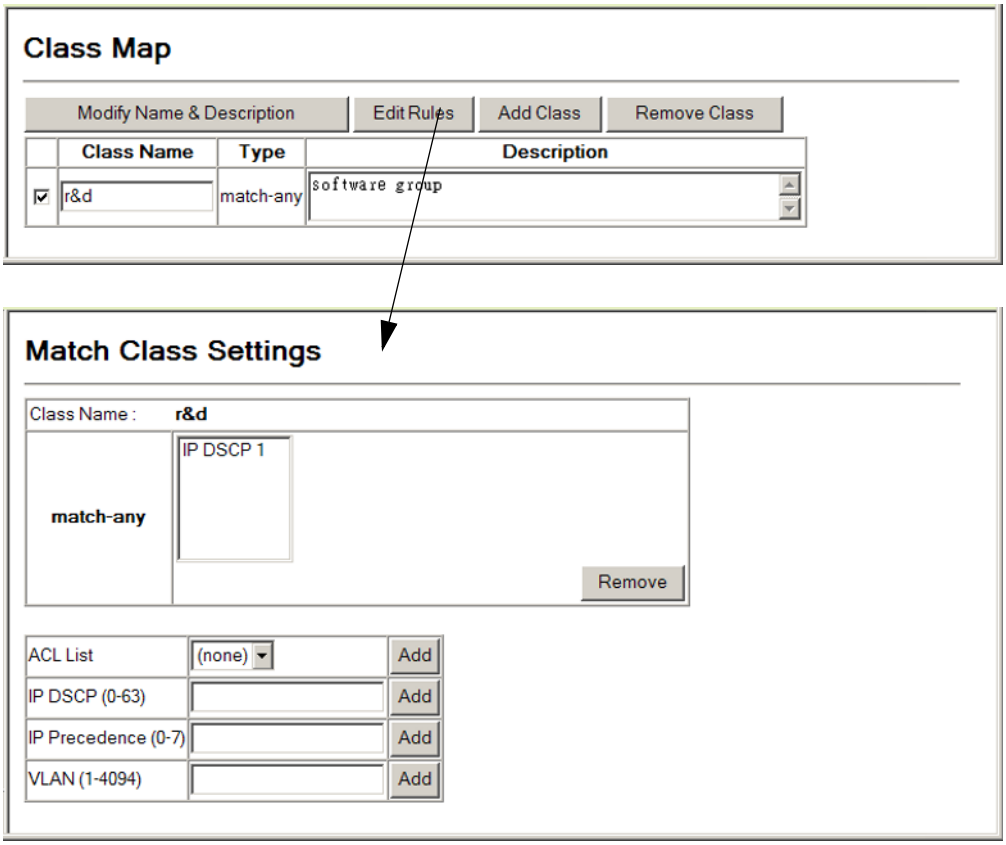
Figure 186: Creating a Class Map



To edit the rules for a class map:

1. Click QoS, DiffServ, Class Map.
2. Select the name of a class map.
3. Click Edit Rules.
4. Specify type of traffic for this class based on an access list, a DSCP or IP Precedence value, or a VLAN. You can specify up to 16 items to match when assigning ingress traffic to a class map.
5. Click Add.

Figure 187: Adding Rules to a Class Map



CREATING QOS POLICIES

Use the QoS > DiffServ > Policy Map page to create a policy map that can be attached to multiple interfaces.

CLI REFERENCES

- "Quality of Service Commands" on page 853

COMMAND USAGE

A policy map is used to group one or more class map statements (page 384), modify service tagging, and enforce bandwidth policing. A policy map can then be bound by a service policy to one or more interfaces (page 391).

Configuring QoS policies requires several steps. A class map must first be configured which indicates how to match the inbound packets according to an access list, a DSCP or IP Precedence value, or a member of specific VLAN. A policy map is then configured which indicates the boundary parameters used for monitoring inbound traffic, and the action to take for non-conforming traffic. A policy map may contain one or more classes based on previously defined class maps.

The class of service can be assigned to matching packets. In addition, the flow rate of inbound traffic can be monitored and the response to non-conforming traffic specified.

- To configure a Policy Map, follow these steps:
  - Create a Class Map as described on page 384.
  - Open the Policy Map page, and click Add Policy.
  - When the Policy Configuration page opens, fill in the "Policy Name" field, and click Add.
  - When the Policy Rule Settings page opens, select a class name from the scroll-down list (Class Name field). Configure a policy for traffic that matches criteria defined in this class by setting the quality of service that an IP packet will receive (in the Action field), defining the maximum throughput and burst rate (in the Meter field), and the action that results from a policy violation (in the Exceed field). Then finally click Add to register the new policy.
- A policy map can contain multiple class statements that can be applied to the same interface with the Service Policy Settings (page 391). You can configure up to 64 policers (i.e., meters or class maps) for each of the following access list types: MAC ACL, IP ACL or IPv6 ACL. Also, note that the maximum number of classes that can be applied to a policy map is 200.

  Policing is based on a token bucket, where bucket depth (i.e., the maximum burst before the bucket overflows) is specified by the "Burst" field, and the average rate at which tokens are removed from the bucket is specified by the "Rate" option.
- After using the policy map to define packet classification, service tagging, and bandwidth policing, it must be assigned to a specific interface by a service policy (page 391) to take effect.

PARAMETERS

These parameters are displayed:

Policy Map

- **Modify Name and Description** – Configures the name and a brief description of a policy map. (Range: 1-16 characters for the name; 1-64 characters for the description)
- **Edit Classes** – Opens the "Policy Rule Settings" page for the selected class entry. Modify the criteria used to service ingress traffic on this page.
- **Add Policy** – Opens the "Policy Configuration" page. Enter a policy name and description on this page, and click Add to open the "Policy Rule Settings" page. Enter the criteria used to service ingress traffic on this page.

- **Remove Policy** – Deletes a specified policy.

Policy Configuration (Add Policy)

- **Policy Name** – Name of policy map. (Range: 1-16 characters)
- **Description** – A brief description of a policy map. (Range: 1-64 characters)
- **Add** – Adds the specified policy.
- **Back** – Returns to previous page with making any changes.

Policy Rule Settings (Edit Classes)

- Class Settings -

- **Policy Name** – Name of policy map.
- **Class Name** – Name of a class map that defines a traffic classification upon which a policy can act.
- **Action** – Shows the service provided to ingress traffic by setting a CoS, DSCP, or IP Precedence value in a matching packet (as specified in Match Class Settings on page 384).
- **Meter** – The maximum throughput and burst rate.
  - **Rate (kbps)** – Rate in kilobits per second.
  - **Burst (byte)** – Burst in bytes.
- **Exceed Action** – Specifies whether the traffic that exceeds the specified rate will be dropped or the DSCP service level will be reduced.
- **Remove Class** – Deletes a class.

- Policy Options -

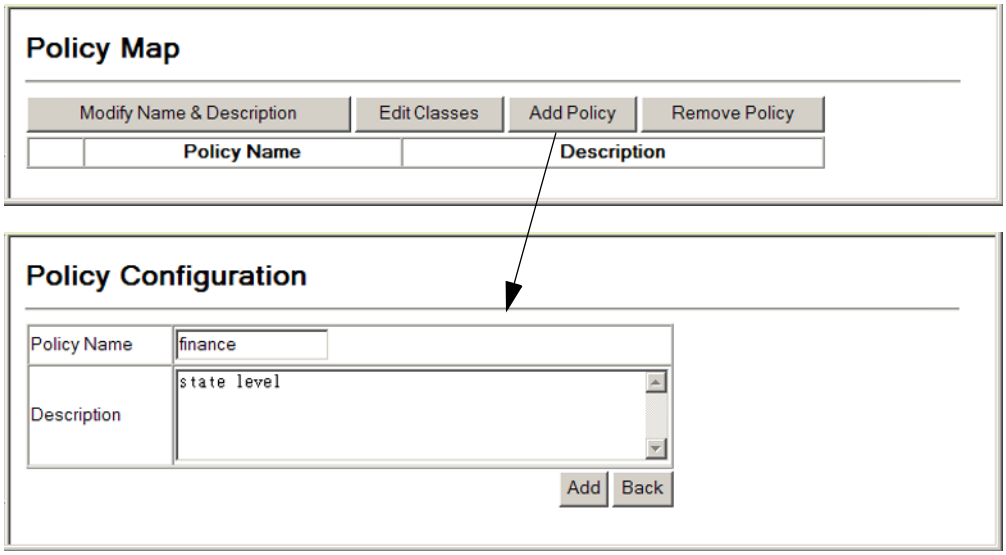
- **Class Name** – Name of class map.
- **Action** – Configures the service provided to ingress traffic by setting a CoS or IP DSCP value in a matching packet (as specified in Match Class Settings on page 384). (Range - CoS: 0-7, DSCP: 0-63)
- **Meter** – Check this to define the maximum throughput, burst rate, and the action that results from a policy violation.
  - **Rate** – Rate in kilobits per second. (Range: 1-100000 kbps or maximum port speed, whichever is lower)
  - **Burst** – Burst in bytes. (Range: 64-524288)

- **Exceed** – Specifies whether the traffic that exceeds the specified rate or burst will be dropped or the DSCP service level will be reduced.
  - **Set** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63).
  - **Drop** – Drops out of conformance traffic.
- **Add** – Adds the specified criteria to the policy map.

WEB INTERFACE

1. Click QoS, DiffServ, Policy Map.
2. Click Add Policy.
3. Enter a policy name and a description.
4. Click Add.

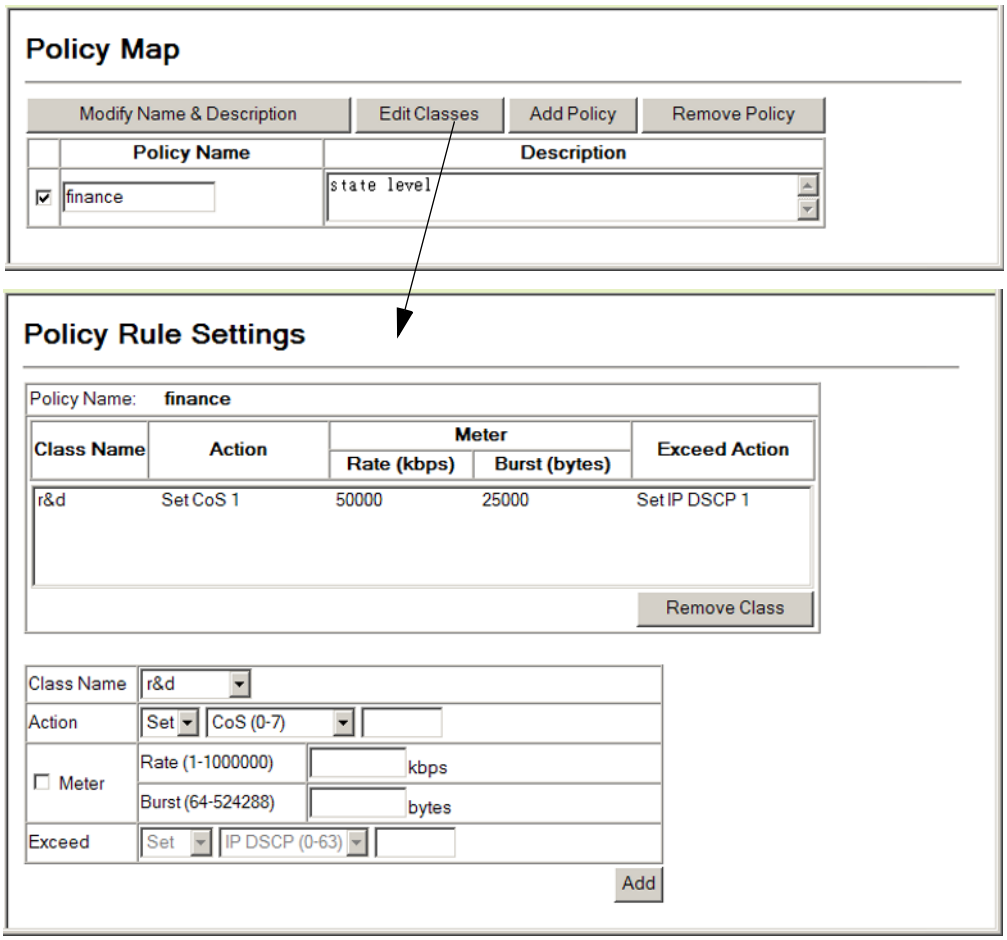
Figure 188: Creating a Policy Map



To edit the rules for a policy map:

1. Click QoS, DiffServ, Policy Map.
2. Select the name of a policy map.
3. Click Edit Rules.
4. Set the CoS or IP DSCP for matching packets to specify the quality of service to be assigned to the matching traffic class. Use metering to define the maximum throughput and burst rate. Then specify the action to take for non-conforming traffic.
5. Click Add.

Figure 189: Adding Rules to a Policy Map



ATTACHING A POLICY MAP TO A PORT

Use the QoS > DiffServ > Service Policy page to bind a policy map to an ingress port.

CLI REFERENCES

- "Quality of Service Commands" on page 853

COMMAND USAGE

- First define a class map, define a policy map, and bind the service policy to the required interface.
- Only one policy map can be bound to an interface.
- The switch does not allow a policy map to be bound to an interface for egress traffic.

PARAMETERS

These parameters are displayed:

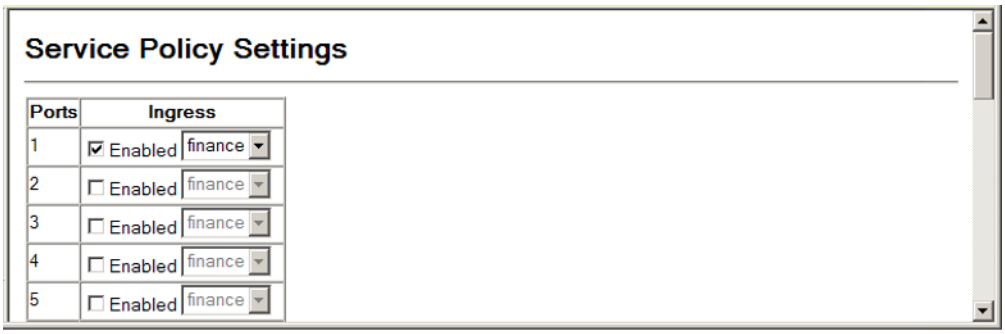
- **Port** – Specifies a port.
- **Ingress** – Applies the selected rule to ingress traffic.
- **Enabled** – Check this to enable a policy map on the specified port.
- *Policy Map* – Select the appropriate policy map from the scroll-down box.

WEB INTERFACE

To bind a policy map to a port:

1. Click QoS, DiffServ, Service Policy.
2. Check the box under the Ingress field to enable a policy map for a port.
3. Select a policy map from the scroll-down box.
4. Click Apply.

Figure 190: Attaching a Policy Map to a Port



16 VoIP Traffic Configuration

This chapter covers the following topics:

- Global Settings – Enables VOIP globally, sets the Voice VLAN, and the aging time for attached ports.
- Port Settings – Configures the way in which a port is added to the Voice VLAN, the filtering of non-VoIP packets, the method of detecting VoIP traffic, and the priority assigned to voice traffic.
- Telephony OUI List – Configures the list of phones to be treated as VOIP devices based on the specified Organization Unit Identifier (OUI).

Overview

When IP telephony is deployed in an enterprise network, it is recommended to isolate the Voice over IP (VoIP) network traffic from other data traffic. Traffic isolation can provide higher voice quality by preventing excessive packet delays, packet loss, and jitter. This is best achieved by assigning all VoIP traffic to a single Voice VLAN.

The use of a Voice VLAN has several advantages. It provides security by isolating the VoIP traffic from other data traffic. End-to-end QoS policies and high priority can be applied to VoIP VLAN traffic across the network, guaranteeing the bandwidth it needs. VLAN isolation also protects against disruptive broadcast and multicast traffic that can seriously affect voice quality.

The switch allows you to specify a Voice VLAN for the network and set a CoS priority for the VoIP traffic. The VoIP traffic can be detected on switch ports by using the source MAC address of packets, or by using LLDP (IEEE 802.1AB) to discover connected VoIP devices. When VoIP traffic is detected on a configured port, the switch automatically assigns the port as a tagged member the Voice VLAN. Alternatively, switch ports can be manually configured.

CONFIGURING VOIP TRAFFIC

Use the QoS > VoIP Traffic Setting > Configuration page to configure the switch for VoIP traffic. First enable automatic detection of VoIP devices attached to the switch ports, then set the Voice VLAN ID for the network. The Voice VLAN aging time can also be set to remove a port from the Voice VLAN when VoIP traffic is no longer received on the port.

CLI REFERENCES

- "Configuring Voice VLANs" on page 837

PARAMETERS

These parameters are displayed:

- **Auto Detection Status** – Enables the automatic detection of VoIP traffic on switch ports. (Default: Disabled)
- **Voice VLAN ID** – Sets the Voice VLAN ID for the network. Only one Voice VLAN is supported and it must already be created on the switch. (Range: 1-4094)
- **Voice VLAN Aging Time** – The time after which a port is removed from the Voice VLAN when VoIP traffic is no longer received on the port. (Range: 5-43200 minutes; Default: 1440 minutes)

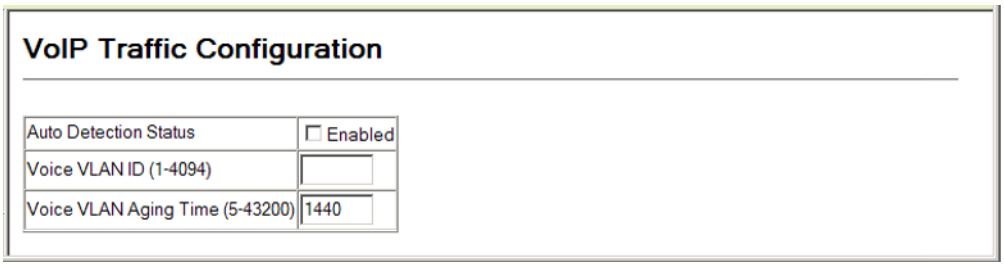
NOTE: The Voice VLAN ID cannot be modified when the global Auto Detection Status is enabled.

WEB INTERFACE

To configure global settings for a Voice VLAN:

1. Click QoS, VoIP Traffic Setting, Configuration.
2. Enable Auto Detection.
3. Specify the Voice VLAN ID.
4. Adjust the Voice VLAN Aging Time if required.
5. Click Apply.

Figure 191: Configuring a Voice VLAN



CONFIGURING VOIP TRAFFIC PORTS

Use the QoS > VoIP Traffic Setting > Port Configuration page to configure ports for VoIP traffic, you need to set the mode (Auto or Manual), specify the discovery method to use, and set the traffic priority. You can also enable security filtering to ensure that only VoIP traffic is forwarded on the Voice VLAN.

CLI REFERENCES

- "Configuring Voice VLANs" on page 837

PARAMETERS

These parameters are displayed:

- **Mode** – Specifies if the port will be added to the Voice VLAN when VoIP traffic is detected. (Default: None)
  - **None** – The Voice VLAN feature is disabled on the port. The port will not detect VoIP traffic or be added to the Voice VLAN.
  - **Auto** – The port will be added as a tagged member to the Voice VLAN when VoIP traffic is detected on the port. You must select a method for detecting VoIP traffic, either OUI or 802.1ab (LLDP). When OUI is selected, be sure to configure the MAC address ranges in the Telephony OUI list.
  - **Manual** – The Voice VLAN feature is enabled on the port, but the port must be manually added to the Voice VLAN.
- **Security** – Enables security filtering that discards any non-VoIP packets received on the port that are tagged with the voice VLAN ID. VoIP traffic is identified by source MAC addresses configured in the Telephony OUI list, or through LLDP that discovers VoIP devices attached to the switch. Packets received from non-VoIP sources are dropped. (Default: Disabled)
- **Discovery Protocol** – Selects a method to use for detecting VoIP traffic on the port. (Default: OUI)
  - **OUI** – Traffic from VoIP devices is detected by the Organizationally Unique Identifier (OUI) of the source MAC address. OUI numbers

are assigned to manufacturers and form the first three octets of a device MAC address. MAC address OUI numbers must be configured in the Telephony OUI list so that the switch recognizes the traffic as being from a VoIP device.

- **802.1ab** – Uses LLDP (IEEE 802.1ab) to discover VoIP devices attached to the port. LLDP checks that the "telephone bit" in the system capability TLV is turned on. See "Link Layer Discovery Protocol" for more information on LLDP.

- **Priority** – Defines a CoS priority for port traffic on the Voice VLAN. The priority of any received VoIP packet is overwritten with the new priority when the Voice VLAN feature is active for the port. (Range: 0-6; Default: 6)

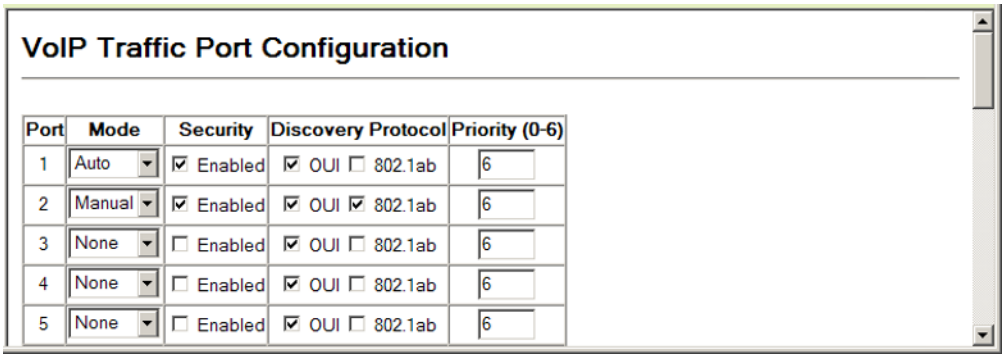
- **Remaining Age** – Number of minutes before this entry is aged out.

WEB INTERFACE

To configure VoIP traffic settings for a port:

1. Click QoS, VoIP Traffic Setting, Port Configuration.
2. Set the mode for a VoIP traffic port, select the detection mechanism to use, and specify the VoIP traffic priority.
3. Click Apply.

Figure 192: Configuring Port Settings for a Voice VLAN



CONFIGURING TELEPHONY OUI

VoIP devices attached to the switch can be identified by the manufacturer's Organizational Unique Identifier (OUI) in the source MAC address of received packets. OUI numbers are assigned to manufacturers and form the first three octets of device MAC addresses. The MAC OUI numbers for VoIP equipment can be configured on the switch so that traffic from these devices is recognized as VoIP. Use the QoS > VoIP Traffic Setting > OUI Configuration page to configure this feature.

CLI REFERENCES

- "Configuring Voice VLANs" on page 837

PARAMETERS

These parameters are displayed:

- **Telephony OUI** – Specifies a MAC address range to add to the list. Enter the MAC address in format 01-23-45-67-89-AB.
- **Mask** – Identifies a range of MAC addresses. Selecting a mask of FF-FF-FF-00-00-00 identifies all devices with the same OUI (the first three octets). Other masks restrict the MAC address range. Selecting FF-FF-FF-FF-FF-FF specifies a single MAC address. (Default: FF-FF-FF-00-00-00)
- **Description** – User-defined text that identifies the VoIP devices.

WEB INTERFACE

To configure MAC OUI numbers for VoIP equipment:

1. Click QoS, VoIP Traffic Setting, OUI Configuration.
2. Enter a MAC address that specifies the OUI for VoIP devices in the network.
3. Select a mask from the pull-down list to define a MAC address range.
4. Enter a description for the devices.
5. Click Add.

Figure 193: Configuring an OUI Telephony List

17 MULTICAST FILTERING

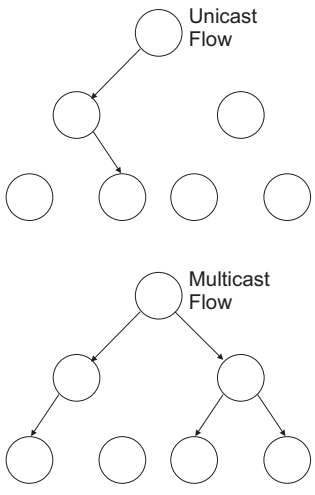
This chapter describes how to configure the following multicast services:

- IGMP – Configuring snooping and query parameters.
- Filtering and Throttling – Filtering specified multicast service, or throttling the maximum of multicast groups allowed on an interface.
- Multicast VLAN Registration (MVR) – Configures a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, preserving security and data isolation.

OVERVIEW

Multicasting is used to support real-time applications such as video conferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts that want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed on to the hosts which subscribed to this service.

Figure 194: Multicast Filtering Concept



This switch can use Internet Group Management Protocol (IGMP) to filter multicast traffic. IGMP Snooping can be used to passively monitor or "snoop" on exchanges between attached hosts and an IGMP-enabled

device, most commonly a multicast router. In this way, the switch can discover the ports that want to join a multicast group, and set its filters accordingly.

If there is no multicast router attached to the local subnet, multicast traffic and query messages may not be received by the switch. In this case (Layer 2) IGMP Query can be used to actively ask the attached hosts if they want to receive a specific multicast service. IGMP Query thereby identifies the ports containing hosts requesting to join the service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

The purpose of IP multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches, instead of flooding traffic to all ports in the subnet (VLAN).

LAYER 2 IGMP (SNOOPING AND QUERY)

IGMP Snooping and Query – If multicast routing is not supported on other switches in your network, you can use IGMP Snooping and IGMP Query (page 401) to monitor IGMP service requests passing between multicast clients and servers, and dynamically configure the switch ports which need to forward multicast traffic. IGMP Snooping conserves bandwidth on network segments where no node has expressed interest in receiving a specific multicast service. For switches that do not support multicast routing, or where multicast routing is already enabled on other switches in the local network segment, IGMP Snooping is the only service required to support multicast filtering.

When using IGMPv3 snooping, service requests from IGMP Version 1, 2 or 3 hosts are all forwarded to the upstream router as IGMPv3 reports. The primary enhancement provided by IGMPv3 snooping is in keeping track of information about the specific multicast sources which downstream IGMPv3 hosts have requested or refused. The switch maintains information about both multicast groups and channels, where a group indicates a multicast flow for which the hosts have *not* requested a specific source (the only option for IGMPv1 and v2 hosts unless statically configured on the switch), and a channel indicates a flow for which the hosts have requested service from a specific source.

Only IGMPv3 hosts can request service from a specific multicast source. When downstream hosts request service from a specific source for a multicast service, these sources are all placed in the Include list, and traffic is forwarded to the hosts from each of these sources. IGMPv3 hosts may also request that service be forwarded from any source except for those specified. In this case, traffic is filtered from sources in the Exclude list, and forwarded from all other available sources.

NOTE: When the switch is configured to use IGMPv3 snooping, the snooping version may be downgraded to version 2 or version 1, depending on the version of the IGMP query packets detected on each VLAN.

NOTE: IGMP snooping will not function unless a multicast router port is enabled on the switch. This can accomplished in one of two ways. A static router port can be manually configured (see "Specifying Static Interfaces for a Multicast Router"). Using this method, the router port is never timed out, and will continue to function until explicitly removed. The other method relies on the switch to dynamically create multicast routing ports whenever multicast routing protocol packets or IGMP query packets are detected on a port.

NOTE: A maximum of up to 255 multicast entries can be maintained for IGMP snooping. If the table's capacity is exceeded, the IGMPv3 snooping will not support multicast source filtering, but will forward multicast traffic from all relevant sources to the requesting hosts.

Static IGMP Router Interface – If IGMP snooping cannot locate the IGMP querier, you can manually designate a known IGMP querier (i.e., a multicast router/switch) connected over the network to an interface on your switch (page 405). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

CONFIGURING IGMP SNOOPING AND QUERY PARAMETERS

Use the IGMP Snooping > IGMP Configuration page to configure the switch to forward multicast traffic. Based on the IGMP query and report messages, the switch forwards multicast traffic only to the ports that request it. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.

CLI REFERENCES

- "IGMP Snooping" on page 865

COMMAND USAGE

- **IGMP Snooping** – This switch can passively snoop on IGMP Query and Report packets transferred between IP multicast routers/switches and IP multicast host groups to identify the IP multicast group members. It simply monitors the IGMP packets passing through it, picks out the group registration information, and configures the multicast filters accordingly.

NOTE: Unknown multicast traffic is flooded to all ports in the VLAN for several seconds when first received. If a multicast router port exists on the VLAN, the traffic will be filtered by subjecting it to IGMP snooping. If no router port exists on the VLAN or the multicast filtering table is already full, the switch will continue flooding the traffic into the VLAN.

- **IGMP Querier** – A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "querier" and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

NOTE: Multicast routers use this information from IGMP snooping and query reports, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

- **IGMP Leave Proxy** – This function is only effective if IGMP snooping is enabled.

  IGMP leave proxy suppresses all unnecessary IGMP leave messages so that the non-querier switch forwards an IGMP leave packet only when the last dynamic member port leaves a multicast group.

  The leave-proxy feature does not function when a switch is set as the querier.

  When the switch a non-querier, the receiving port is not the last dynamic member port in the group, the receiving port is not a router port, and no IGMPv1 member port exists in the group, the switch will generate and send a GS-query to the member port which received the leave message, and then start the last member query timer for that port.

  When the conditions in the preceding item all apply, except that the receiving port is a router port, then the switch will not send a GS-query, but will immediately start the last member query timer for that port.

PARAMETERS

These parameters are displayed:

- **IGMP Status** – When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is referred to as IGMP Snooping. (Default: Enabled)
- **Act as IGMP Querier** – When enabled, the switch can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic. This feature is not supported for IGMPv3 snooping. (Default: Disabled)
- **Leave Proxy Status** – Suppresses leave messages unless received from the last member port in the group. (Default: Disabled)
- **IGMP Query Count** – Sets the maximum number of queries issued for which there has been no response before the switch takes action to drop a client from the multicast group. (Range: 2-10; Default: 2)
- **IGMP Query Interval** – Sets the frequency at which the switch sends IGMP host-query messages. (Range: 60-125 seconds; Default: 125)

- **IGMP Report Delay** – Sets the time between receiving an IGMP Report for an IP multicast address on a port before the switch sends an IGMP Query out of that port and removes the entry from its list. (Range: 5-25 seconds; Default: 10)

- **IGMP Query Timeout** – The time the switch waits after the previous querier stops before it considers it to have expired. (Range: 1-65535, Recommended Range: 300-500 seconds, Default: 300)

- **IGMP Version** – Sets the protocol version for compatibility with other devices on the network. This is the IGMP Version the switch uses to send snooping reports. (Range: 1-3; Default: 2)

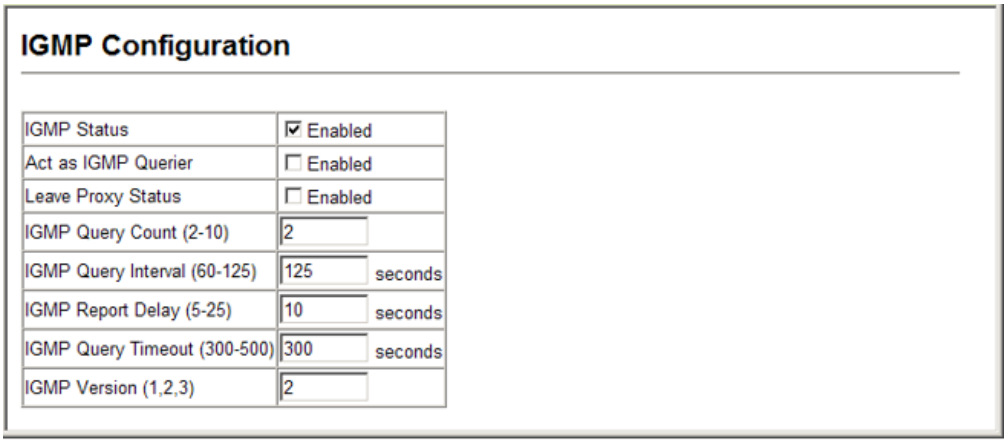
  This attribute configures the IGMP report/query version used by IGMP snooping. Versions 1 - 3 are all supported, and versions 2 and 3 are backward compatible, so the switch can operate with other devices, regardless of the snooping version employed.

WEB INTERFACE

To configure general settings for IGMP Snooping and Query:

1. Click IGMP Snooping > IGMP Configuration.
2. Adjust the IGMP settings as required.
3. Click Apply.

Figure 195: Configuring General Settings for IGMP Snooping



ENABLING IGMP IMMEDIATE LEAVE

Use the IGMP Snooping > IGMP Immediate Leave page to immediately delete a member port of a multicast service if a leave packet is received at that port and the immediate-leave function is enabled for the parent VLAN. This allows the switch to remove a port from the multicast forwarding table without first having to send an IGMP group-specific query to that interface.

CLI REFERENCES

- "ip igmp snooping immediate-leave" on page 869

COMMAND USAGE

- If immediate leave is *not* used, a multicast router (or querier) will send a group-specific query message when an IGMPv2/v3 group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period. Note that the timeout period is determined by the IGMP Query Report Delay (see "Configuring IGMP Snooping and Query Parameters" on "Configuring IGMP Snooping and Query Parameters").

- If immediate leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one IGMP-enabled device, either a service host or a neighbor running IGMP snooping.

- Immediate leave is only effective if IGMP snooping is enabled, and IGMPv2 or IGMPv3 snooping is used.

- Immediate leave does not apply to a port if the switch has learned that a multicast router is attached to it.

- Immediate leave can improve bandwidth usage for a network which frequently experiences many IGMP host add and leave requests.

PARAMETERS

These parameters are displayed:

- **VLAN ID** – VLAN Identifier. (Range: 1-4094).

- **Immediate Leave** – Sets the status for immediate leave on the specified VLAN. (Default: Disabled)

WEB INTERFACE

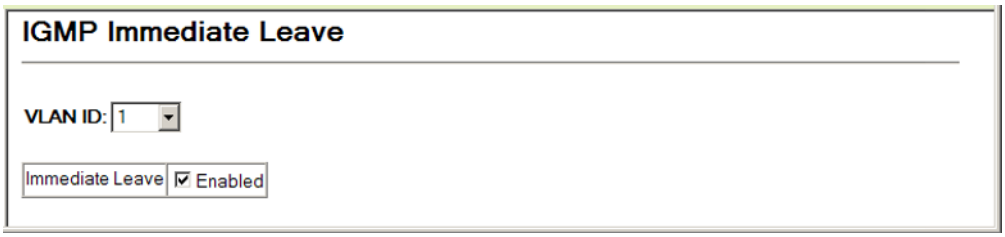
To immediately delete a member port of a multicast service if a leave packet is received:

1. Click IGMP Snooping, IGMP Immediate Leave.

2. Select the VLAN which will forward all the corresponding multicast traffic, and set the status for immediate leave.

3. Click Apply.

Figure 196: Enabling IGMP Immediate Leave



DISPLAYING INTERFACES ATTACHED TO A MULTICAST ROUTER

Multicast routers that are attached to ports on the switch use information obtained from IGMP, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet. These routers may be dynamically discovered by the switch or statically assigned to an interface on the switch. Use the IGMP Snooping > Multicast Router Port Information page to display the interfaces on this switch that are statically attached to a neighboring multicast router/switch.

CLI REFERENCES

- "show ip igmp snooping" on page 870

PARAMETERS

These parameters are displayed:

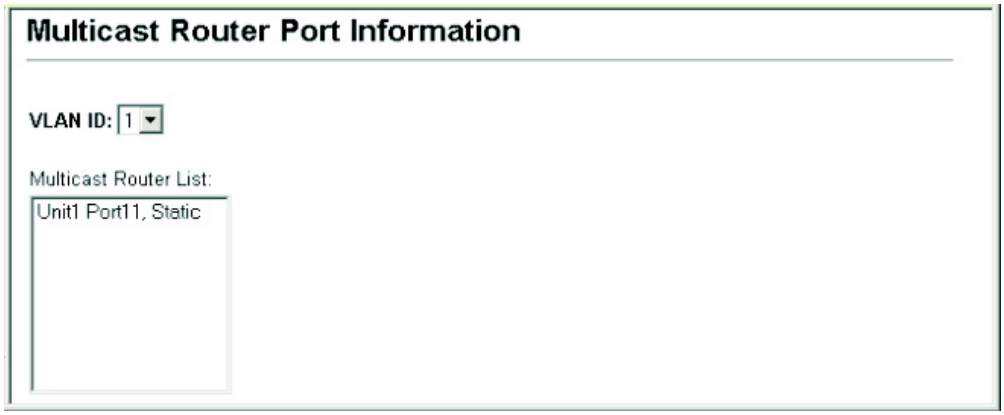
- **VLAN ID** – ID of configured VLAN (1-4094).
- **Multicast Router List** – Multicast routers dynamically discovered by this switch or those that are statically assigned to an interface on this switch.

WEB INTERFACE

To show the static interfaces attached to a multicast router:

1. Click IGMP Snooping, Multicast Router Port Information.
2. Select the VLAN for which to display this information.

Figure 197: Showing Static Interfaces Attached a Multicast Router



SPECIFYING STATIC INTERFACES FOR A MULTICAST ROUTER

Use the IGMP Snooping > Static Multicast Router Port Configuration page to statically attach an interface to a multicast router/switch.

Depending on network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on the switch, the interface (and a specified VLAN) can be manually configured to join all the current multicast groups supported by the

attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the switch.

CLI REFERENCES

- "Static Multicast Routing" on page 875

PARAMETERS

These parameters are displayed:

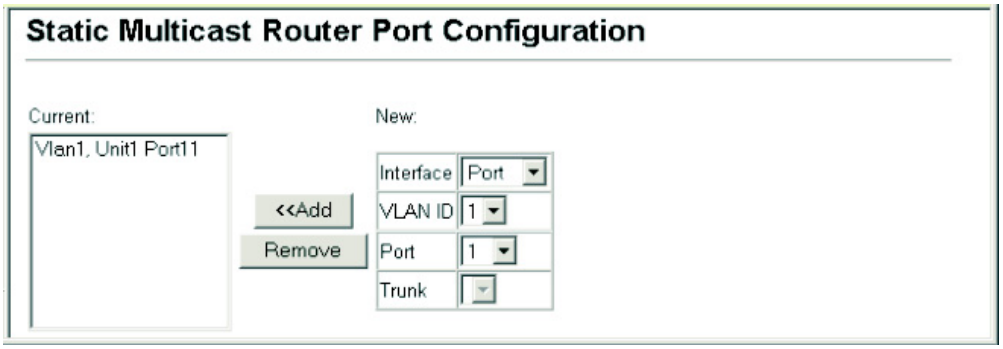
- **Interface** – Activates the Port or Trunk scroll down list.
- **VLAN ID** – Selects the VLAN which is to propagate all multicast traffic coming from the attached multicast router. (Range: 1-4094)
- **Port** or **Trunk** – Specifies the interface attached to a multicast router.

WEB INTERFACE

To specify a static interface attached to a multicast router:

1. Click IGMP Snooping, Multicast Router Port Configuration.
2. Select the port or trunk attached to the multicast router, and the VLAN which will forward all the corresponding multicast traffic.
3. Click Apply.

Figure 198: Configuring a Static Interface for a Multicast Router



DISPLAYING PORT MEMBERS OF MULTICAST SERVICES

Use the IGMP Snooping > IP Multicast Registration Table to display the port members associated with a specified VLAN and multicast service.

CLI REFERENCES

- "show mac-address-table multicast" on page 871

PARAMETERS

These parameters are displayed:

- **VLAN ID** – Selects the VLAN for which to display port members. (Range: 1-4094)

- **Multicast IP Address** – The IP address for a specific multicast service.
- **Multicast Group Port List** – Shows the interfaces that have already been assigned to the selected VLAN to propagate a specific multicast service.

WEB INTERFACE

To display the port members associated with a specified VLAN and multicast service:

1. IGMP Snooping, IP Multicast Registration Table.
2. Select the VLAN for which to display this information.
3. Select the IP address for a multicast service.

Figure 199: Showing Port Members of Multicast Services

ASSIGNING INTERFACES TO MULTICAST SERVICES

Use the IGMP Snooping > IGMP Member Port Table to statically assign a multicast service to an interface.

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages (see "Configuring IGMP Snooping and Query Parameters"). However, for certain applications that require tighter control, it may be necessary to statically configure a multicast service on the switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

CLI REFERENCES

- "ip igmp snooping vlan static" on page 868

COMMAND USAGE

- Static multicast addresses are never aged out.

- When a multicast address is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

PARAMETERS

These parameters are displayed:

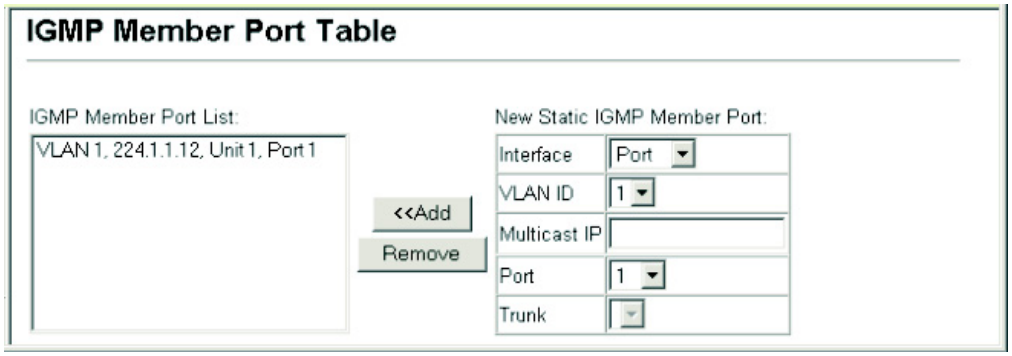
- **Interface** – Activates the Port or Trunk scroll down list.
- **VLAN ID** – Specifies the VLAN which is to propagate the multicast service. (Range: 1-4094)
- **Multicast IP** – The IP address for a specific multicast service.
- **Port** or **Trunk** – Specifies the interface assigned to a multicast group.

WEB INTERFACE

To statically assign an interface to a multicast service:

1. Click IGMP Snooping, IGMP Member Port Table.
2. specify the interface attached to a multicast service (through an IGMP-enabled switch or multicast router), select the VLAN that will propagate the multicast service, and enter the multicast IP address.
3. Click Apply.

Figure 200: Assigning an Interface to a Multicast Service



FILTERING AND THROTTLING IGMP GROUPS

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The IGMP filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and IGMP throttling limits the number of simultaneous multicast groups a port can join.

IGMP filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. An IGMP filter

profile can contain one or more addresses, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, IGMP join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the IGMP join report is forwarded as normal. If a requested multicast group is denied, the IGMP join report is dropped.

IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either "deny" or "replace." If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

NOTE: IGMP filtering and throttling only applies to dynamically learned multicast groups. It does not apply to statically configured groups.

ENABLING IGMP FILTERING AND THROTTLING

Use the IGMP Snooping > IGMP Filter Configuration page to enable IGMP filtering and throttling globally on the switch.

CLI REFERENCES

- "ip igmp filter (Global Configuration)" on page 878

COMMAND USAGE

To implement IGMP filtering and throttling on the switch, you must first enable the feature globally and create IGMP profile numbers.

PARAMETERS

These parameters are displayed:

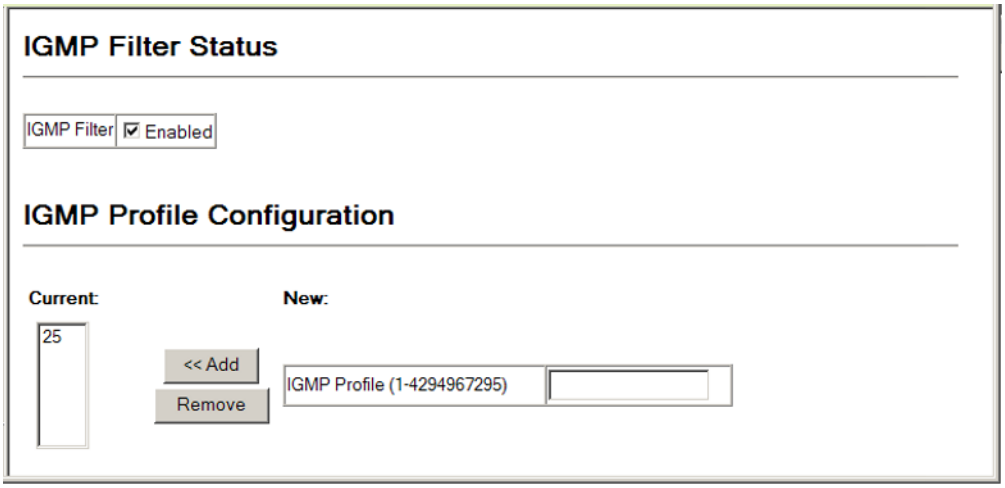
- **IGMP Filter** – Enables IGMP filtering and throttling globally for the switch. (Default: Disabled)
- **IGMP Profile** – Creates an IGMP profile. (Range: 1-4294967295)

WEB INTERFACE

To enable IGMP filtering and throttling on the switch:

1. Click IGMP Snooping, IGMP Filter Configuration.
2. Create a profile group by entering a number in the text box and clicking Add.
3. Enable IGMP Filter Status, and click Apply.

Figure 201: Enabling IGMP Filtering and Throttling



CONFIGURING IGMP FILTER PROFILES

Use the IGMP Snooping > IGMP Filter Profile Configuration page to set the access mode and multicast groups to filter for an IGMP profile.

CLI REFERENCES

- "IGMP Filtering and Throttling" on page 877

COMMAND USAGE

Specify a range of multicast groups by entering a start and end IP address; or specify a single multicast group by entering the same IP address for the start and end of the range.

PARAMETERS

These parameters are displayed:

- **Profile ID** – Creates an IGMP profile. (Range: 1-4294967295)
- **Access Mode** – Sets the access mode of the profile; either permit or deny. (Default: Deny)

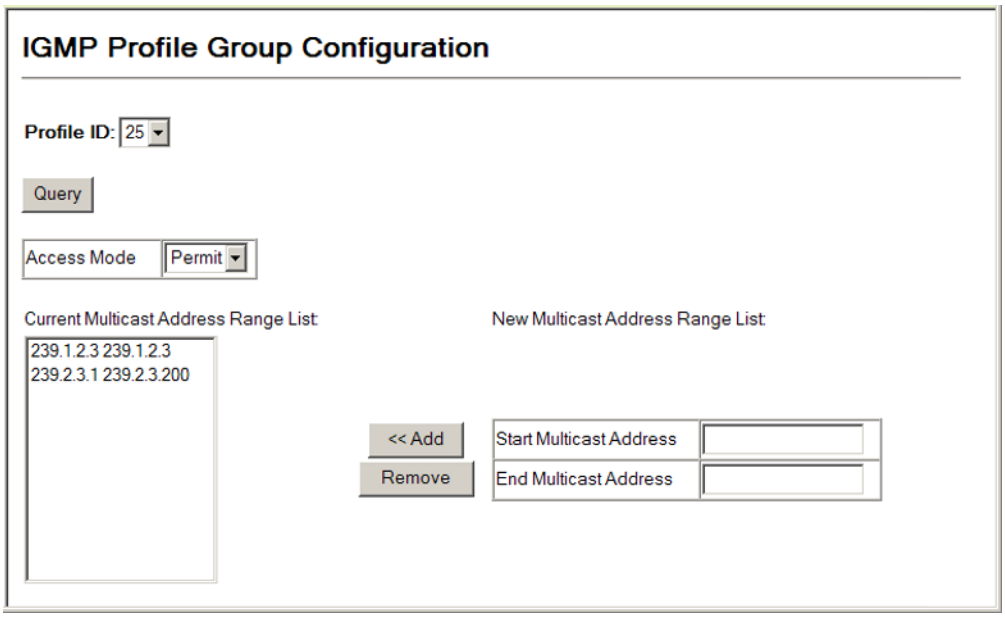
  When the access mode is set to permit, IGMP join reports are processed when a multicast group falls within the controlled range. When the access mode is set to deny, IGMP join reports are only processed when the multicast group is not in the controlled range.
- **Start Multicast IP Address** – Specifies the starting address of a range of multicast groups.
- **End Multicast IP Address** – Specifies the ending address of a range of multicast groups.

WEB INTERFACE

To configure an IGMP filter profile:

1. Click IGMP Snooping, IGMP Filter Profile Configuration.
2. Select the profile number you want to configure, and click Query to display the current settings.
3. Specify the access mode for the profile and then add multicast groups to the profile list.
4. Click Apply.

Figure 202: Configuring an IGMP Filtering Profile



CONFIGURING IGMP FILTERING AND THROTTLING FOR INTERFACES

Use the IGMP Snooping > IGMP Filter and Throttling Port Configuration or Trunk Configuration page to assign and IGMP filter profile to interfaces on the switch, or to throttle multicast traffic by limiting the maximum number of multicast groups an interface can join at the same time.

CLI REFERENCES

- "IGMP Filtering and Throttling" on page 877

COMMAND USAGE

IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

PARAMETERS

These parameters are displayed:

- *Interface* – Port or trunk identifier.

  An IGMP profile or throttling setting can be applied to a port or trunk. When ports are configured as trunk members, the trunk uses the settings applied to the first port member in the trunk.

- **Profile** – Selects an existing profile to assign to an interface.

- **Max Multicast Groups** – Sets the maximum number of multicast groups an interface can join at the same time. (Range: 0-256; Default: 256)

- **Current Multicast Groups** – Displays the current multicast groups the interface has joined.

- **Throttling Action Mode** – Sets the action to take when the maximum number of multicast groups for the interface has been exceeded. (Default: Deny)
  - **deny** - The new multicast group join report is dropped.
  - **replace** - The new multicast group replaces an existing group.

- **Throttling Status** – Indicates if the throttling action has been implemented on the interface. (Options: True or False)

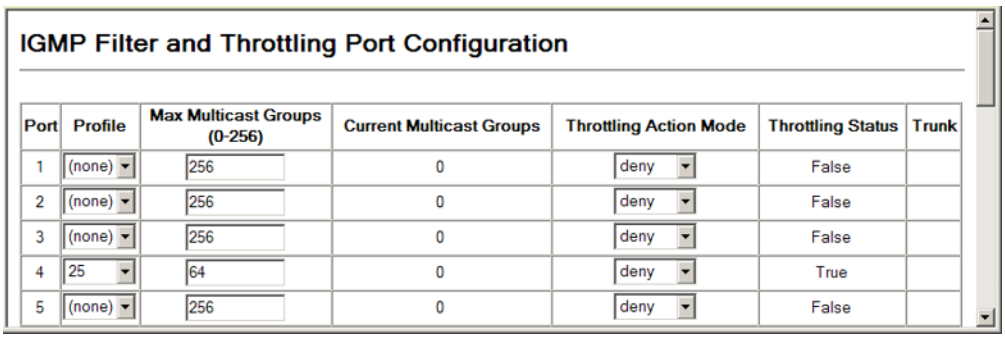
- **Trunk** – Indicates if a port is a trunk member.

WEB INTERFACE

To configure IGMP filtering or throttling for a port or trunk:

1. Click IGMP Snooping, IGMP Filter/Throttling Port Configuration or Trunk Configuration.
2. Select a profile to assign to an interface, then set the maximum number of allowed multicast groups and the throttling response.
3. Click Apply.

Figure 203: Configuring IGMP Filtering and Throttling Interface Settings

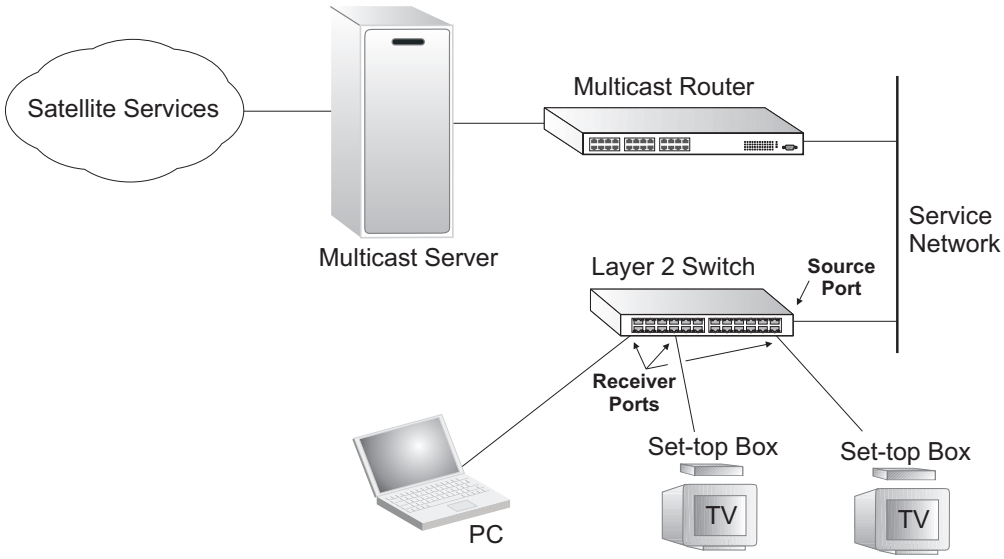


MULTICAST VLAN REGISTRATION

Multicast VLAN Registration (MVR) is a protocol that controls access to a single network-wide VLAN most commonly used for transmitting multicast traffic (such as television channels or video-on-demand) across a service provider's network. Any multicast traffic entering an MVR VLAN is sent to all attached subscribers. This protocol can significantly reduce to processing overhead required to dynamically monitor and establish the distribution tree for a normal multicast VLAN. This makes it possible to support common multicast services over a wide part of the network without having to use any multicast routing protocol.

MVR maintains the user isolation and data security provided by VLAN segregation by passing only multicast traffic into other VLANs to which the subscribers belong. Even though common multicast streams are passed onto different VLAN groups from the MVR VLAN, users in different IEEE 802.1Q or private VLANs cannot exchange any information (except through upper-level routing services).

Figure 204: MVR Concept



COMMAND USAGE

- General Configuration Guidelines for MVR:

1. Enable MVR globally on the switch, select the MVR VLAN, and add the multicast groups that will stream traffic to attached hosts (see "Configuring Global MVR Settings").
2. Set the interfaces that will join the MVR as source ports or receiver ports (see "Configuring MVR Interface Status" on page 417).
3. For multicast streams that will run for a long term and be associated with a stable set of hosts, you can statically bind the multicast group to the participating interfaces (see "Assigning Static Multicast Groups to Interfaces").

- Although MVR operates on the underlying mechanism of IGMP snooping, the two features operate independently of each other. One can be enabled or disabled without affecting the behavior of the other. However, if IGMP snooping and MVR are both enabled, MVR reacts only to join and leave messages from multicast groups configured under MVR. Join and leave messages from all other multicast groups are managed by IGMP snooping. Also, note that only IGMP version 2 or 3 hosts can issue multicast join or leave messages.

CONFIGURING GLOBAL MVR SETTINGS

Use the MVR > Configuration page to enable MVR globally on the switch, select the VLAN that will serve as the sole channel for common multicast streams supported by the service provider, and assign the multicast group address for each of these services to the MVR VLAN.

CLI REFERENCES

- "Multicast VLAN Registration" on page 884

COMMAND USAGE

IGMP snooping and MVR share a maximum number of 255 groups. Any multicast streams received in excess of this limitation will be flooded to all ports in the associated VLAN.

PARAMETERS

These parameters are displayed:

- **MVR Status** – When MVR is enabled on the switch, any multicast data associated with an MVR group is sent from all designated source ports, to all receiver ports that have registered to receive data from that multicast group. (Default: Disabled)

- **MVR Running Status** – Indicates whether or not all necessary conditions in the MVR environment are satisfied. Running status is Active as long as MVR is enabled, the specified MVR VLAN exists, and a source port with a valid link has been configured (see "Configuring MVR Interface Status").

- **MVR VLAN** – Identifier of the VLAN that serves as the channel for streaming multicast services using MVR. MVR source ports should be configured as members of the MVR VLAN (see "Adding Static Members to VLANs"), but MVR receiver ports should not be manually configured as members of this VLAN. (Default: 1)

- **MVR Group IP** – IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255; Default: no groups are assigned to the MVR VLAN)

  Any multicast data sent to this address is sent to all source ports on the switch and all receiver ports that have elected to receive data on that multicast address.

  The IP address range of 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.

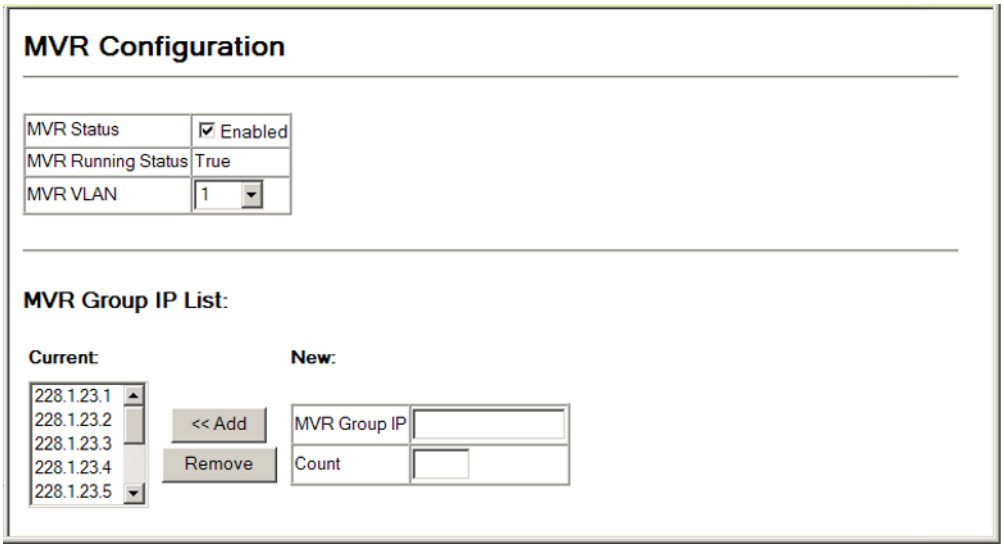
- **Count** – The number of contiguous MVR group addresses. (Range: 1-255; Default: 0)

WEB INTERFACE

To configure global settings for MVR:

1. Click MVR, Configuration.
2. Enable MVR globally on the switch, select the MVR VLAN, and then click Apply.
3. Enter the multicast groups that will stream traffic to participating hosts, and click Add to register each group.

Figure 205: Configuring Global Settings for MVR



DISPLAYING MVR INTERFACE STATUS

Use the MVR > Port Information or Trunk Information page to display information about the interfaces attached to the MVR VLAN.

CLI REFERENCES

- "show mvr" on page 893

PARAMETERS

These parameters are displayed:

- **Type** – Shows the MVR port type.
- **Oper Status** – Shows the link status.
- **MVR Status** – Shows the MVR status. MVR status for source ports is "Active" if MVR is globally enabled on the switch. MVR status for receiver ports is "Active" only if there are subscribers receiving multicast traffic from one of the MVR groups, or a multicast group has been statically assigned to an interface.

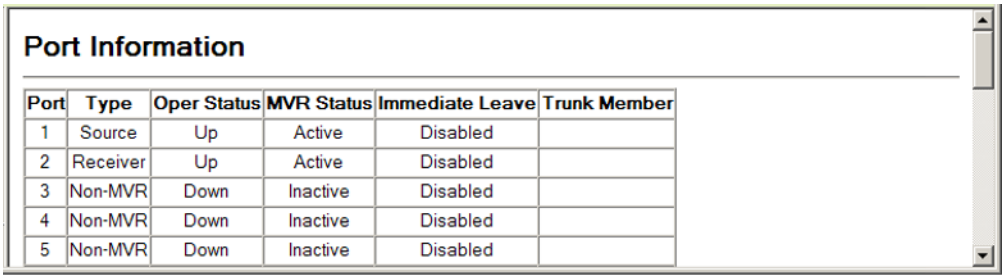
- **Immediate Leave** – Shows if immediate leave is enabled or disabled.
- **Trunk Member**[12] – Shows if port is a trunk member.

WEB INTERFACE

To display information about the interfaces attached to the MVR VLAN:

1. Click MVR, Port Information or Trunk Information.

Figure 206: Displaying MVR Interface Status



DISPLAYING PORT MEMBERS OF MULTICAST GROUPS

Use the MVR > Group IP Information page to display the multicast groups assigned to the MVR VLAN either through IGMP snooping or static configuration.

CLI REFERENCES

- "show mvr" on page 893

PARAMETERS

These parameters are displayed:

- **Group IP** – Multicast groups assigned to the MVR VLAN.
- **Group Port List** – Shows the interfaces with subscribers for multicast services provided through the MVR VLAN.

12. Port Information only.

WEB INTERFACE

To display the multicast groups assigned to the MVR VLAN:

1. Click MVR, Group IP Information.

Figure 207: Displaying Port Members of Multicast Groups

CONFIGURING MVR INTERFACE STATUS

Use the MVR > Port Configuration or Trunk Configuration page to configure each interface that participates in the MVR protocol as a source port or receiver port. If you are sure that only one subscriber attached to an interface is receiving multicast services, you can enable the immediate leave function.

CLI REFERENCES

- "Multicast VLAN Registration" on page 884

COMMAND USAGE

- A port configured as an MVR receiver or source port can join or leave multicast groups configured under MVR. However, note that these ports can also use IGMP snooping to join or leave any other multicast groups using the standard rules for multicast filtering.

- Receiver ports can belong to different VLANs, but should not be configured as a member of the MVR VLAN. IGMP snooping is used to allow a receiver port to dynamically join or leave multicast groups within an MVR VLAN. Multicast groups can also be statically assigned to a receiver port (see "Assigning Static Multicast Groups to Interfaces").

  Receiver ports should not be statically configured as a member of the MVR VLAN. If so configured, its MVR status will be inactive.

  Also, note that VLAN membership for MVR receiver ports cannot be set to trunk mode (see "Configuring VLAN Attributes for Interfaces").

- One or more interfaces may be configured as MVR source ports. A source port is able to both receive and send data for configured MVR groups or for groups which have been statically assigned (see "Assigning Static Multicast Groups to Interfaces").

  All source ports must belong to the MVR VLAN.

Subscribers should not be directly connected to source ports.

- Immediate leave applies only to receiver ports. When enabled, the receiver port is immediately removed from the multicast group identified in the leave message. When immediate leave is disabled, the switch follows the standard rules by sending a group-specific query message to the receiver port and waiting for a response to determine if there are any remaining subscribers for that multicast group before removing the port from the group list.
  - Using immediate leave can speed up leave latency, but should only be enabled on a port attached to one multicast subscriber to avoid disrupting services to other group members attached to the same interface.
  - Immediate leave does not apply to multicast groups which have been statically assigned to a port.

PARAMETERS

These parameters are displayed:

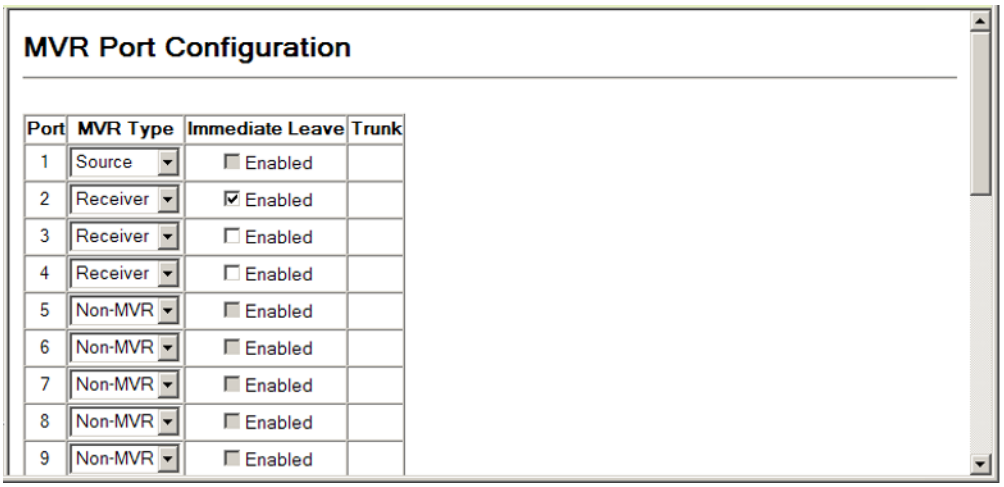
- **Port** – Port identifier.
- **MVR Type** – The following interface types are supported:
  - **Source** – An uplink port that can send and receive multicast data for the groups assigned to the MVR VLAN. Note that the source port must be manually configured as a member of the MVR VLAN (see "Adding Static Members to VLANs").
  - **Receiver** – A subscriber port that can receive multicast data sent through the MVR VLAN. Any port configured as an receiver port will be dynamically added to the MVR VLAN when it forwards an IGMP report or join message from an attached host requesting any of the designated multicast services supported by the MVR VLAN. Just remember that only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned (see "Assigning Static Multicast Groups to Interfaces").
  - **Non-MVR** – An interface that does not participate in the MVR VLAN. (This is the default type.)
- **Oper. Status** – Shows the link status.
- **Immediate Leave** – Configures the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group. (This option only applies to an interface configured as an MVR receiver.)

WEB INTERFACE

To configure interface settings for MVR:

1. Click MVR, Port Configuration or Trunk Configuration.
2. Set each port that will participate in the MVR protocol as a source port or receiver port, and optionally enable Immediate Leave on any receiver port to which only one subscriber is attached.
3. Click Apply.

Figure 208: Configuring Interface Settings for MVR



ASSIGNING STATIC MULTICAST GROUPS TO INTERFACES

Use the MVR > Group Member Configuration page to statically bind multicast groups to a port which will receive long-term multicast streams associated with a stable set of hosts.

CLI REFERENCES

- "mvr group" on page 889

COMMAND USAGE

- Any multicast groups that use the MVR VLAN must be statically assigned to it under the MVR Configuration menu (see"Configuring Global MVR Settings").
- The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.

PARAMETERS

These parameters are displayed:

- **Interface** – Indicates a port or trunk.
- **Member** – Shows the IP addresses for MVR multicast groups which have been statically assigned to the selected interface.

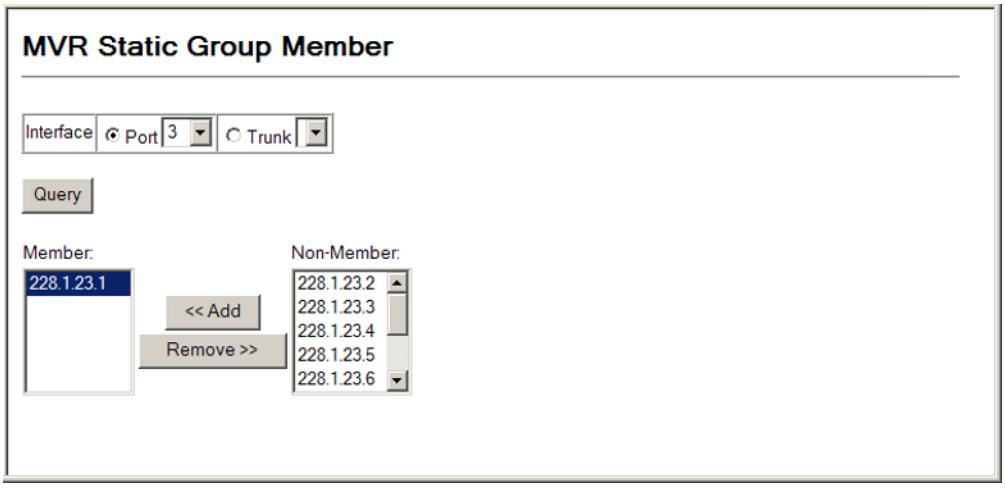
- **Non-Member** – Shows the IP addresses for all MVR multicast groups which have not been statically assigned to the selected interface.

WEB INTERFACE

To assign a static MVR group to a port:

1. Click MVR, Group Member Configuration.
2. Select a port or trunk from the "Interface" field, and click Query to display the assigned multicast groups.
3. Select a multicast address from the displayed lists, and click the Add or Remove button to modify the Member list.

Figure 209: Assigning Static MVR Groups to a Port



CONFIGURING MVR RECEIVER VLAN AND GROUP ADDRESSES

Multicast traffic forwarded to subscribers is normally stripped of frame tags to prevent hosts from discovering the identity of the MVR VLAN. An MVR Receiver VLAN and the multicast services supported by this VLAN can be configured to hide the MVR VLAN, while allowing multicast traffic with frame tags to be forwarded to subscribers.

If a port is manually assigned to the receiver VLAN as a tagged member, multicast traffic forwarded to the subscriber will also carry tags.

Use the MVR > Receiver Configuration page to configure the MVR Receiver VLAN and assigned multicast addresses.

PARAMETERS

These parameters are displayed:

- **MVR Receiver VLAN** – Allows multicast traffic to be forwarded from the specified Receiver VLAN without revealing the identity of the MVR VLAN in tagged frames. (Range: 1-4094)

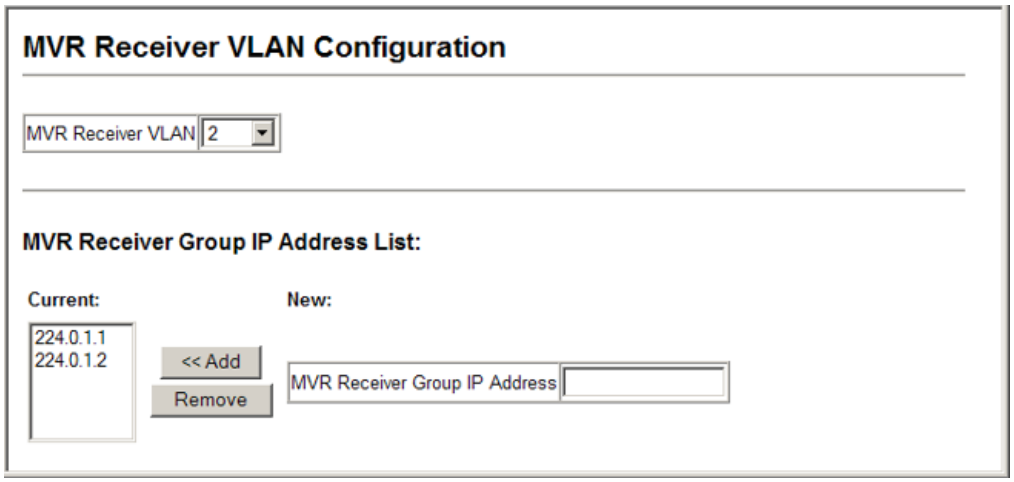
- **MVR Receiver Group IP Address** – Specifies groups to be managed through the receiver VLAN.

WEB INTERFACE

To configure the MVR Receiver VLAN and assigned addresses:

1. Click MVR, Receiver Configuration.
2. Select a VLAN from the MVR Receiver VLAN list.
3. Enter the required multicast groups in the member list, and then click the Add or Remove button to modify the list.

Figure 210: Configuring MVR Receiver VLAN and Group Addresses



DISPLAYING MVR RECEIVER GROUPS

Use the MVR > Receiver Group IP Information page to display the interfaces assigned to the MVR receiver groups.

CLI REFERENCES

- "show mvr" on page 893

PARAMETERS

These parameters are displayed:

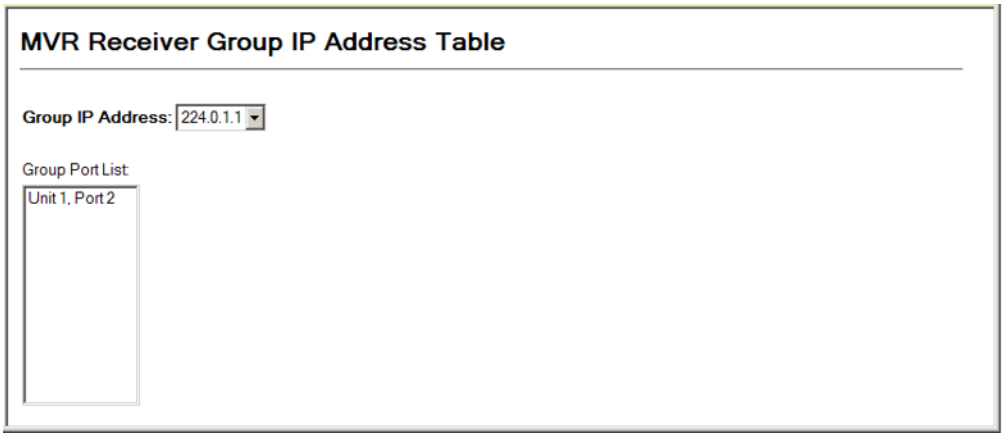
- **Group IP Address** – Multicast groups assigned to the MVR VLAN.
- **Group Port List** – Shows the interfaces with subscribers for multicast services provided through the MVR Receiver VLAN.

WEB INTERFACE

To display the interfaces assigned to the MVR receiver groups:

1. Click Multicast, Receiver Group IP Information.
2. Select a receiver group multicast address from the Group IP Address list to show the interfaces which have joined the selected group.

Figure 211: Displaying MVR Receiver Groups



CONFIGURING STATIC MVR RECEIVER GROUP MEMBERS

Use the MVR > Receiver Group Member Configuration page to statically assign a multicast receiver group to the selected interface.

CLI REFERENCES

- "mvr static-receiver-group" on page 891

PARAMETERS

These parameters are displayed:

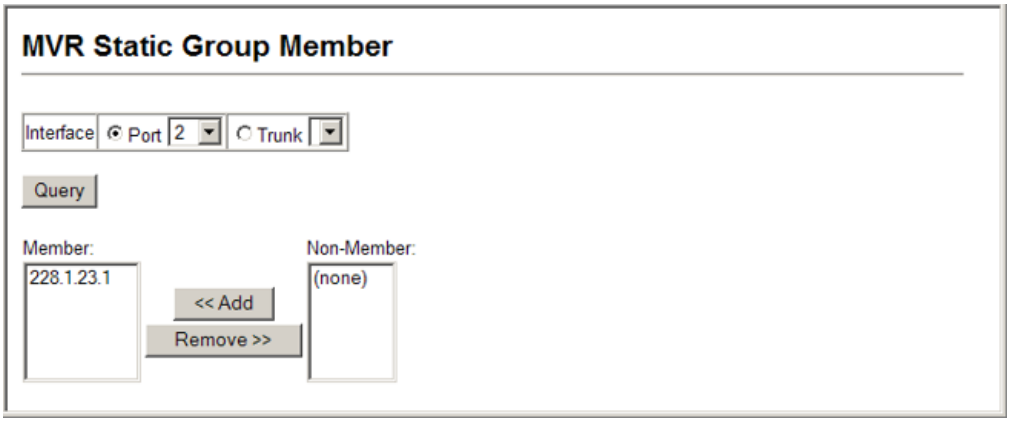
- **Interface** – Indicates a port or trunk.
- **Member List** – Multicast receiver groups assigned to the selected interface. Note that the displayed multicast services have been configured as a receiver group to be managed through the MVR receiver VLAN (see "Configuring MVR Receiver VLAN and Group Addresses").

WEB INTERFACE

To statically assign a multicast receiver group to the selected interface:

1. Click Multicast, Receiver Group Member Configuration.
2. Select a port or trunk from the Interface list, and click Query.
3. Select a multicast group address from the member list, and then click Add or Remove to modify the list.

Figure 212: Configuring Static MVR Receiver Group Members



18 DOMAIN NAME SERVICE

Domain Name Service (DNS) on this switch allows host names to be mapped to IP addresses using static table entries or by redirection to other name servers on the network. When a client device designates this switch as a DNS server, the client will attempt to resolve host names into IP addresses by forwarding DNS queries to the switch, and waiting for a response.

You can manually configure entries in the DNS table used for mapping domain names to IP addresses, configure default domain names, or specify one or more name servers to use for domain name to address translation.

CONFIGURING GENERAL DNS SERVICE PARAMETERS

Use the DNS > General Configuration page to enable domain lookup and set the default domain name.

CLI REFERENCES

- "ip domain-lookup" on page 928
- "ip domain-name" on page 929

COMMAND USAGE

- To enable DNS service on this switch, first configure one or more name servers, and then enable domain lookup status.
- To append domain names to incomplete host names received from a DNS client (i.e., not formatted with dotted notation), you can specify a default domain name or a list of domain names to be tried in sequential order.
- If there is no domain list, the default domain name is used. If there is a domain list, the system will search it for a corresponding entry. If none is found, the default domain name is used.
- When an incomplete host name is received by the DNS service on this switch and a domain name list has been specified, the switch will work through the domain list, appending each domain name in the list to the host name, and checking with the specified name servers for a match.
- When more than one name server is specified, the servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.
- Note that if all name servers are deleted, DNS will automatically be disabled.

PARAMETERS

These parameters are displayed:

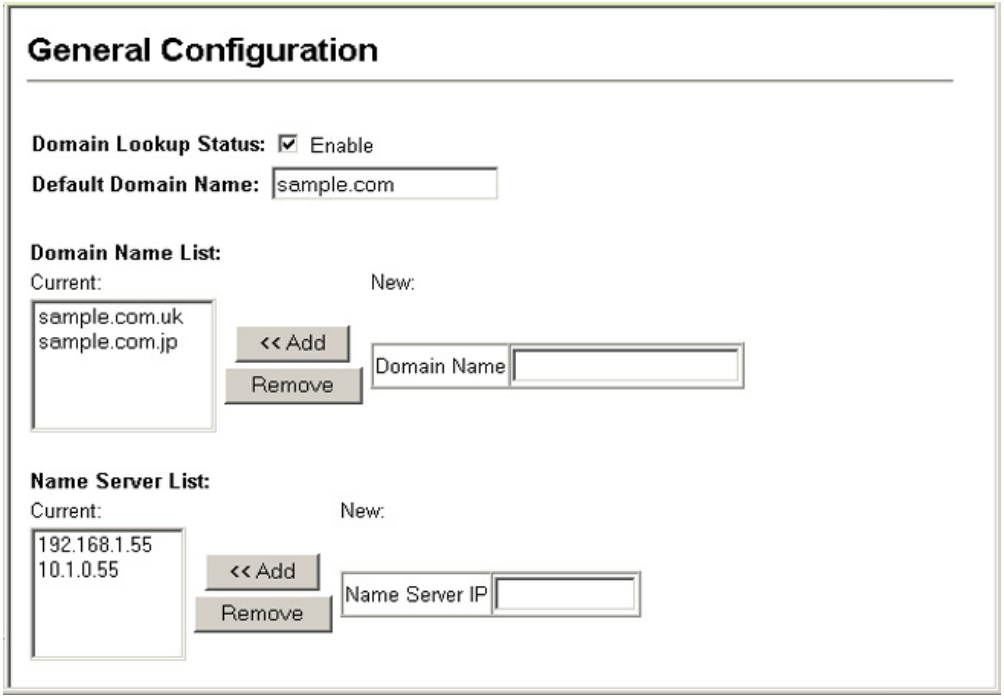
- **Domain Lookup Status** – Enables DNS host name-to-address translation. (Default: Enabled)
- **Default Domain Name**[13] – Defines the default domain name appended to incomplete host names. (Range: 1-64 alphanumeric characters)
- **Domain Name List**[13] – Defines a list of domain names that can be appended to incomplete host names. (Range: 1-64 alphanumeric characters. 1-5 names)
- **Name Server List** – Specifies the address of one or more domain name servers to use for name-to-address resolution. (Range: 1-6 IP addresses)

WEB INTERFACE

To configure general settings for DNS:

1. Click DNS, General Configuration.
2. Enable domain lookup status, set the default domain name or list of domain names, and specify one or more name servers to use to use for address resolution.
3. Click Apply.

Figure 213: Configuring General Settings for DNS



13. Do not include the initial dot that separates the host name from the domain name.

CONFIGURING STATIC DNS HOST TO ADDRESS ENTRIES

Use the DNS > Static Host Table page to manually configure static entries in the DNS table that are used to map domain names to IP addresses.

CLI REFERENCES

- "ip host" on page 930
- "show hosts" on page 934

COMMAND USAGE

- Static entries may be used for local devices connected directly to the attached network, or for commonly used resources located elsewhere on the network.

- Servers or other network devices may support one or more connections via multiple IP addresses. If more than one IP address is associated with a host name in the static table or via information returned from a name server, a DNS client can try each address in succession, until it establishes a connection with the target device.

PARAMETERS

These parameters are displayed:

- **Host Name** – Name of a host device that is mapped to one or more IP addresses. (Range: 1-64 characters)

- **IP Address** – Internet address(es) associated with a host name. (Range: 1-8 addresses)

WEB INTERFACE

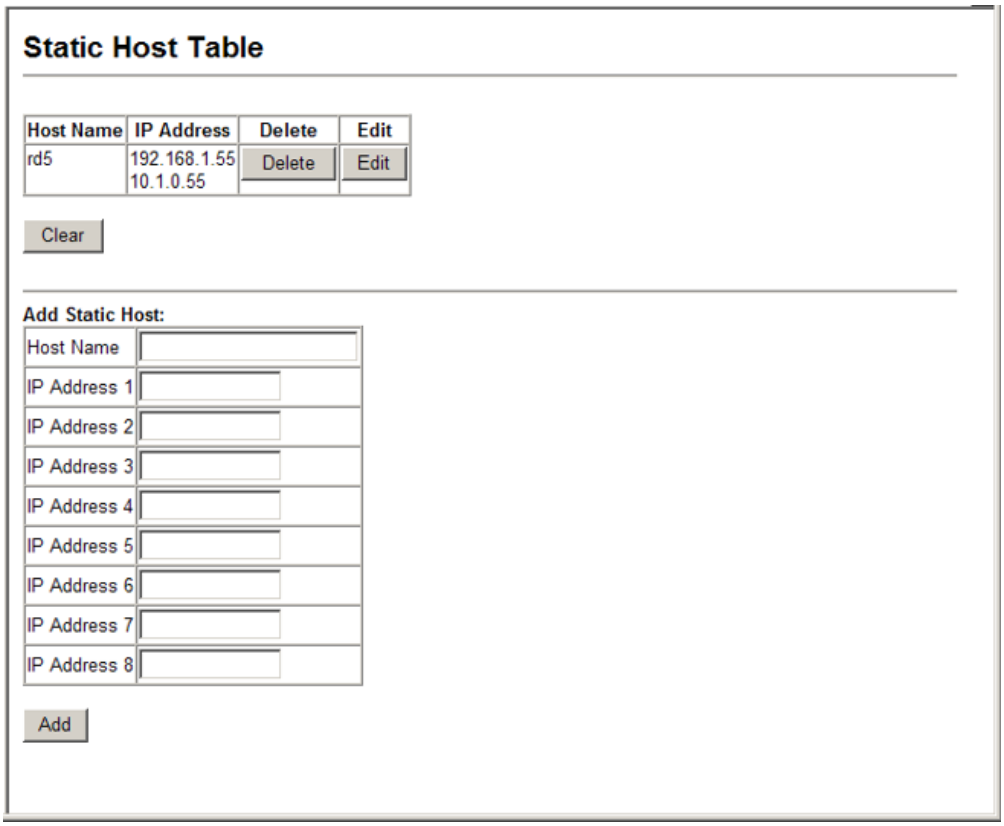
To configure static entries in the DNS table:

1. Click DNS, Static Host Table.

2. Enter a host name and the corresponding address.

3. Click Add.

Figure 214: Configuring Static Entries in the DNS Table



DISPLAYING THE DNS CACHE

Use the DNS - Cache page to display entries in the DNS cache that have been learned via the designated name servers.

CLI REFERENCES

- "show dns cache" on page 933

PARAMETERS

These parameters are displayed:

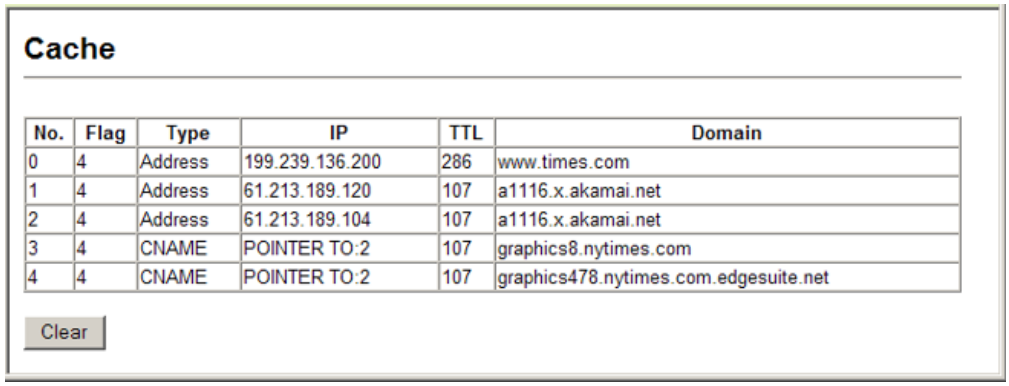
- **No.** – The entry number for each resource record.
- **Flag** – The flag is always "4" indicating a cache entry and therefore unreliable.
- **Type** – This field includes CNAME which specifies the host address for the owner, and ALIAS which specifies an alias.
- **IP** – The IP address associated with this record.
- **TTL** – The time to live reported by the name server.
- **Domain** – The domain name associated with this record.

WEB INTERFACE

To display entries in the DNS cache:

1. Click DNS, Cache.

Figure 215: Showing Entries in the DNS Cache



SECTION III

COMMAND LINE INTERFACE

This section provides a detailed description of the Command Line Interface, along with examples for all of the commands.

This section includes these chapters:

19 USING THE COMMAND LINE INTERFACE

This chapter describes how to use the Command Line Interface (CLI).

ACCESSING THE CLI

When accessing the management interface for the switch over a direct connection to the server's console port, or via a Telnet or Secure Shell connection (SSH), the switch can be managed by entering command keywords and parameters at the prompt. Using the switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

CONSOLE CONNECTION

To access the switch through the console port, perform these steps:

1. At the console prompt, enter the user name and password. (The default user names are "admin" and "guest" with corresponding passwords of "admin" and "guest.") When the administrator user name and password is entered, the CLI displays the "Console#" prompt and enters privileged access mode (i.e., Privileged Exec). But when the guest user name and password is entered, the CLI displays the "Console>" prompt and enters normal access mode (i.e., Normal Exec).

2. Enter the necessary commands to complete your desired tasks.

3. When finished, exit the session with the "quit" or "exit" command.

After connecting to the system through the console port, the login screen displays:

```
User Access Verification
Username: admin
Password:
  CLI session with the ES3528M is opened.
  To end the CLI session, enter [Exit].
Console#
```

TELNET CONNECTION

Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion. For example, the IP address assigned to this switch, 10.1.0.1, consists of a network portion (10.1.0) and a host portion (1).

NOTE: The IP address for this switch is obtained via DHCP by default.

To access the switch through a Telnet session, you must first set the IP address for the Master unit, and set the default gateway if you are managing the switch from a different IP subnet. For example,

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.254 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
Console(config)#
```

If your corporate network is connected to another network outside your office or to the Internet, you need to apply for a registered IP address. However, if you are attached to an isolated network, then you can use any IP address that matches the network segment to which you are attached.

After you configure the switch with an IP address, you can open a Telnet session by performing these steps:

1. From the remote host, enter the Telnet command and the IP address of the device you want to access.
2. At the prompt, enter the user name and system password. The CLI will display the "Vty-*n*#" prompt for the administrator to show that you are using privileged access mode (i.e., Privileged Exec), or "Vty-*n*>" for the guest to show that you are using normal access mode (i.e., Normal Exec), where *n* indicates the number of the current Telnet session.
3. Enter the necessary commands to complete your desired tasks.
4. When finished, exit the session with the "quit" or "exit" command.

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:

  CLI session with the ES3528M is opened.
  To end the CLI session, enter [Exit].

Vty-0#
```

NOTE: You can open up to four sessions to the device via Telnet.

ENTERING COMMANDS

This section describes how to enter CLI commands.

KEYWORDS AND ARGUMENTS

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command "show interfaces status ethernet 1/5," **show interfaces** and **status** are keywords, **ethernet** is an argument that specifies the interface type, and **1/5** specifies the unit/port.

You can enter commands as follows:

- To enter a simple command, enter the command keyword.
- To enter multiple commands, enter each command in the required order. For example, to enable Privileged Exec command mode, and display the startup configuration, enter:

```
Console>enable
Console#show startup-config
```

- To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
Console(config)#username admin password 0 smith
```

MINIMUM ABBREVIATION

The CLI will accept a minimum number of characters that uniquely identify a command. For example, the command "configure" can be entered as **con**. If an entry is ambiguous, the system will prompt for further input.

COMMAND COMPLETION

If you terminate input with a Tab key, the CLI will print the remaining characters of a partial keyword up to the point of ambiguity. In the "logging history" example, typing **log** followed by a tab will result in printing the command up to "**logging**."

GETTING HELP ON COMMANDS

You can display a brief description of the help system by entering the **help** command. You can also display command syntax by using the "?" character to list keywords or parameters.

SHOWING COMMANDS

If you enter a "?" at the command prompt, the system will display the first level of keywords or command groups. You can also display a list of valid keywords for a specific command. For example, the command "**system ?**" displays a list of possible system commands:

```
Console#show ?
  access-group          Access groups
  access-list           Access lists
  accounting            Uses an accounting list with this name
  arp                   Information of ARP cache
  auto-traffic-control  Auto traffic control information
  banner                Banner info
  bridge-ext            Bridge extension information
  cable-diagnostics     Shows the information of cable diagnostics
  calendar              Date and time information
  class-map             Displays class maps
  cluster               Display cluster
  debug                 State of each debugging option
  dns                   DNS information
  dot1q-tunnel          dot1q-tunnel
  dot1x                 802.1X content
  eaps                  Displays EAPS infomation
  erps                  Displays ERPS configuration
  garp                  GARP properties
  gvrp                  GVRP interface information
  history               Shows history information
  hosts                 Host information
  interfaces            Shows interface information
  ip                    IP information
  ipv6                  IPv6 information
  l2protocol-tunnel     Layer 2 protocol tunneling configuration
  lacp                  LACP statistics
  line                  TTY line information
  lldp                  LLDP
  log                   Log records
  logging               Logging setting
  mac                   MAC access list
  mac-address-table     Configuration of the address table
  mac-vlan              MAC-based VLAN information
  management            Shows management information
  map                   Maps priority
  memory                Memory utilization
  mvr                   multicast vlan registration
  network-access        Shows the entries of the secure port.
  ntp                   Network Time Protocol configuration
  policy-map            Displays policy maps
  port                  Port characteristics
  pppoe                 Displays PPPoE configuration
  privilege             Shows current privilege level
  process               Device process
  protocol-vlan         Protocol-VLAN information
  public-key            Public key information
  pvlan                 Shows the Private VLAN information
  queue                 Priority queue information
  radius-server         RADIUS server information
  reload                Shows the reload settings
  running-config        Information on the running configuration
```

```
  sflow                 Shows the sflow information
  snmp                  Simple Network Management Protocol statistics
  snmp-server           Displays SNMP server configuration
  sntp                  Simple Network Time Protocol configuration
  spanning-tree         Spanning-tree configuration
  ssh                   Secure shell server connections
  startup-config        Startup system configuration
  subnet-vlan           IP subnet-based VLAN information
  system                System information
  tacacs-server         TACACS server information
  tech-support          Technical information
  time-range            Time range
  upgrade               Shows upgrade information
  upnp                  UPnP settings
  users                 Information about users logged in
  version               System hardware and software versions
  vlan                  Shows virtual LAN settings
  voice                 Shows the voice VLAN information
  web-auth              Shows web authentication configuration
Console#show
```

The command "**show interfaces ?**" will display the following information:

```
Console#show interfaces ?
  brief        brief interface description
  counters       Interface counters information
  status         Shows interface status
  switchport     Shows interface switchport information
  transceiver  Interface of transceiver information
Console#
```

Show commands which display more than one page of information (e.g., **show running-config**) pause and require you to press the [Space] bar to continue displaying one more page, the [Enter] key to display one more line, or the [a] key to display the rest of the information without stopping. You can press any other key to terminate the display.

PARTIAL KEYWORD LOOKUP

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and question mark.) For example "**s?**" shows all the keywords starting with "s."

```
Console#show s?
sflow           snmp            snmp-server     sntp            spanning-tree
ssh             startup-config  subnet-vlan     system

Console#show s
```

NEGATING THE EFFECT OF COMMANDS

For many configuration commands you can enter the prefix keyword "**no**" to cancel the effect of a command or reset the configuration to the default value. For example, the **logging** command will log system messages to a host server. To disable logging, specify the **no logging** command. This guide describes the negation effect for all applicable commands.

USING COMMAND HISTORY

The CLI maintains a history of commands that have been entered. You can scroll back through the history of commands by pressing the up arrow key. Any command displayed in the history list can be executed again, or first modified and then executed.

Using the **show history** command displays a longer list of recently executed commands.

UNDERSTANDING COMMAND MODES

The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain switching functions. These classes are further divided into different modes. Available commands depend on the selected mode. You can always enter a question mark "**?**" at the prompt to display a list of the commands available for the current mode. The command classes and associated modes are displayed in the following table:

Table 31: General Command Modes

Class	Mode	
Exec	Normal Privileged	
Configuration	Global*	Access Control List Class Map EAPS ERPS IGMP Profile Interface Line Multiple Spanning Tree Policy Map Server Group Time Range VLAN Database

* You must be in Privileged Exec mode to access the Global configuration mode. You must be in Global Configuration mode to access any of the other configuration modes.

EXEC COMMANDS

When you open a new console session on the switch with the user name and password "guest," the system enters the Normal Exec command mode (or guest mode), displaying the "Console>" command prompt. Only a limited number of the commands are available in this mode. You can access all commands only from the Privileged Exec command mode (or administrator mode). To access Privilege Exec mode, open a new console

session with the user name and password "admin." The system will now display the "Console#" command prompt. You can also enter Privileged Exec mode from within Normal Exec mode, by entering the enable command, followed by the privileged level password "super."

To enter Privileged Exec mode, enter the following user names and passwords:

```
Username: admin
Password: [admin login password]

  CLI session with the ES3510MA is opened.
  To end the CLI session, enter [Exit].

Console#
```

```
Username: guest
Password: [guest login password]

  CLI session with the ES3510MA is opened.
  To end the CLI session, enter [Exit].

Console>enable
Password: [privileged level password]
Console#
```

CONFIGURATION COMMANDS

Configuration commands are privileged level commands used to modify switch settings. These commands modify the running configuration only and are not saved when the switch is rebooted. To store the running configuration in non-volatile storage, use the **copy running-config startup-config** command.

The configuration commands are organized into different modes:

- Access Control List Configuration - These commands are used for packet filtering.
- Class Map Configuration - Creates a DiffServ class map for a specified traffic type.
- EAPS Configuration - These commands configure Automatic Ethernet Protection Switching for increased availability of Ethernet rings commonly used in service provider networks.
- ERPS Configuration – These commands configure G.8032 Ethernet Ring Protection Switching for increased availability of Ethernet rings commonly used in service provider networks.
- Global Configuration - These commands modify the system level configuration, and include commands such as **hostname** and **snmp-server community**.

- IGMP Profile - Sets a profile group and enters IGMP filter profile configuration mode.
- Interface Configuration - These commands modify the port configuration such as **speed-duplex** and **negotiation**.
- Line Configuration - These commands modify the console port and Telnet configuration, and include command such as **parity** and **databits**.
- Multiple Spanning Tree Configuration - These commands configure settings for the selected multiple spanning tree instance.
- Policy Map Configuration - Creates a DiffServ policy map for multiple interfaces.
- Server Group Configuration - Adds AAA security servers to defined lists.
- Time Range - Sets a time range for use by other functions, such as Access Control Lists.
- VLAN Configuration - Includes the command to create VLAN groups.

To enter the Global Configuration mode, enter the command **configure** in Privileged Exec mode. The system prompt will change to "Console(config)#" which gives you access privilege to all Global Configuration commands.

```
Console#configure
Console(config)#
```

To enter the other modes, at the configuration prompt type one of the following commands. Use the **exit** or **end** command to return to the Privileged Exec mode.

Table 32: Configuration Command Modes

Mode	Command	Prompt	Page
Line	line {console | vty}	Console(config-line)	482
Access Control List	access-list arp	Console(config-arp-acl)	677
	access-list ip standard	Console(config-std-acl)	660
	access-list ip extended	Console(config-ext-acl)	660
	access-list ipv6 standard	Console(config-std-ipv6-acl)	667
	access-list ipv6 extended	Console(config-ext-ipv6-acl)	667
	access-list mac	Console(config-mac-acl)	672
Class Map	class-map	Console(config-cmap)	854
EAPS	eaps domain	Console(config-eaps)	777
ERPS	erps domain	Console(config-erps)	785
Interface	interface {ethernet *port* | port-channel *id*| vlan *id*}	Console(config-if)	682
MSTP	spanning-tree mst-configuration	Console(config-mstp)	750

Table 32: Configuration Command Modes (Continued)

Mode	Command	Prompt	Page
Policy Map	policy-map	Console(config-pmap)	857
Server Group	aaa group server {radius | tacacs+}	Console(config-sg-radius) Console(config-sg-tacacs+)	571
Time Range	time-range	Console(config-time-range)	515
VLAN	vlan database	Console(config-vlan)	805

For example, you can use the following commands to enter interface configuration mode, and then return to Privileged Exec mode

```
Console(config)#interface ethernet 1/5
.
.
.
Console(config-if)#exit
Console(config)#
```

COMMAND LINE PROCESSING

Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the "?" character to display a list of possible matches. You can also use the following editing keystrokes for command-line processing:

Table 33: Keystroke Commands

Keystroke	Function
Ctrl-A	Shifts cursor to start of command line.
Ctrl-B	Shifts cursor to the left one character.
Ctrl-C	Terminates the current task and displays the command prompt.
Ctrl-E	Shifts cursor to end of command line.
Ctrl-F	Shifts cursor to the right one character.
Ctrl-K	Deletes all characters from the cursor to the end of the line.
Ctrl-L	Repeats current command line on a new line.
Ctrl-N	Enters the next command line in the history buffer.
Ctrl-P	Enters the last command.
Ctrl-R	Repeats current command line on a new line.
Ctrl-U	Deletes from the cursor to the beginning of the line.
Ctrl-W	Deletes the last word typed.
Esc-B	Moves the cursor back one word.
Esc-D	Deletes from the cursor to the end of the word.
Esc-F	Moves the cursor forward one word.
Delete key or backspace key	Erases a mistake when entering a command.

OUTPUT MODIFIERS AND REDIRECTION

Many of the show commands include options for output modifiers. For example, the "show ip interface" command includes the following keyword options:

```
Console#show ip interface ?
  |  Output modifiers
  <cr>

Console#show ip interface
```

The output modifiers include options which indicate a string that occurs at the beginning of a line, in lines that are to be excluded, or in lines that are to be included.

```
Console#show ip interface | ?
  begin    Begin with the line that matches
  exclude  Exclude lines that match
  include  Include lines that match
Console#show ip interface |
```

Note: The output modifier begin can only be used as the first modifier if more than one modifier is used in a command.

CLI COMMAND GROUPS

The system commands can be broken down into the functional groups shown below.

Table 34: Command Group Index

Command Group	Description	Page
General	Basic commands for entering privileged access mode, restarting the system, or quitting the CLI	445
System Management	Display and setting of system information, basic modes of operation, maximum frame size, file management, console port and telnet settings, system logs, SMTP alerts, system clock, switch clustering, and UPnP	453
Simple Network Management Protocol	Activates authentication failure traps; configures community access strings, and trap receivers	527
Flow Sampling	Samples traffic flows, and forwards data to designated collector	545
Authentication	Configures user names and passwords, logon access using local or remote authentication (including AAA), management access through the web server, Telnet server and Secure Shell; as well as port security, IEEE 802.1X port access control, restricted access based on specified IP addresses, and PPPoE Intermediate Agent	553

Table 34: Command Group Index (Continued)

Command Group	Description	Page
General Security Measures	Segregates traffic for clients attached to common data ports; and prevents unauthorized access by configuring valid static or dynamic addresses, web authentication, MAC address authentication, filtering DHCP requests and replies, and discarding invalid ARP responses	613
Access Control List	Provides filtering for IPv4 frames (based on address, protocol, TCP/UDP port number, TCP control code, ARP request/response packets), IPv6 frames (based on address or DSCP traffic class), or non-IP frames (based on MAC address or Ethernet type)	659
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs	681
Link Aggregation	Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks	701
Mirror Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port or VLAN	713
Rate Limit	Controls the maximum rate for traffic transmitted or received on a port	717
Automatic Traffic Control	Configures bounding thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port	719
Generic Loopback Detection	Configures detection of loopback conditions caused by hardware problems or faulty protocol settings	733
Address Table	Configures the address table for filtering specified addresses, displays current entries, clears the table, or sets the aging time	739
Spanning Tree	Configures Spanning Tree settings for the switch	743
Ethernet Automatic Protection Switching	Configures EAPS for increased availability of Ethernet rings commonly used in service provider networks	771
Ethernet Ring Protection Switching	Configures G.8032 ERPS for increased availability of Ethernet rings commonly used in service provider networks	785
VLANs	Configures VLAN settings, and defines port membership for VLAN groups; also enables or configures private VLANs, protocol VLANs, IP-subnet VLANs, MAC-based VLANs, voice VLANs, and QinQ tunneling	799
Class of Service	Sets port priority for untagged frames, selects strict priority or weighted round robin, relative weight for each priority queue, also sets priority for DSCP	845
Quality of Service	Configures Differentiated Services classification criteria and service policies	853
Multicast Filtering	Configures IGMP multicast filtering, query, profile; specifies ports attached to a multicast router; also configures multicast VLAN registration	865
MLD Snooping	Configures Multicast Listener Discovery for IPv6 traffic	897
Link Layer Discovery Protocol	Configures LLDP settings to enable information discovery about neighbor devices	905
Domain Name Service	Configures DNS services.	927
Dynamic Host Configuration Protocol	Configures DHCP client functions	935
IP Interface	Configures IP address for the switch	943

The access mode shown in the following tables is indicated by these abbreviations:

ACL (Access Control List Configuration)
CM (Class Map Configuration)
EAPS (EAPS Configuration)
ERPS (ERPS Configuration)
GC (Global Configuration)
IC (Interface Configuration)
IPC (IGMP Profile Configuration)
LC (Line Configuration)
MST (Multiple Spanning Tree)
NE (Normal Exec)
PE (Privileged Exec)
PM (Policy Map Configuration)
SG (Server Group)
TR (Time Range Configuration)
VC (VLAN Database Configuration)

20 GENERAL COMMANDS

These commands are used to control the command access mode, configuration mode, and other basic functions.

Table 35: General Commands

Command	Function	Mode
prompt	Customizes the CLI prompt	GC
reload	Restarts the system at a specified time, after a specified delay, or at a periodic interval	GC
enable	Activates privileged mode	NE
quit	Exits a CLI session	NE, PE
show history	Shows the command history buffer	NE, PE
configure	Activates global configuration mode	PE
disable	Returns to normal mode from privileged mode	PE
reload	Restarts the system immediately	PE
show reload	Displays the current reload settings, and the time at which next scheduled reload will take place	PE
end	Returns to Privileged Exec mode	any config. mode
exit	Returns to the previous configuration mode, or exits the CLI	any mode
help	Shows how to use help	any mode
?	Shows options for command completion (context sensitive)	any mode

prompt

This command customizes the CLI prompt. Use the **no** form to restore the default prompt.

SYNTAX

prompt *string*

no prompt

string - Any alphanumeric string to use for the CLI prompt. (Maximum length: 255 characters)

DEFAULT SETTING

Console

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#prompt RD2
RD2(config)#
```

reload (Global Configuration)

This command restarts the system at a specified time, after a specified delay, or at a periodic interval. You can reboot the system immediately, or you can configure the switch to reset after a specified amount of time. Use the **cancel** option to remove a configured setting.

SYNTAX

reload {**at** *hour minute* [{*month day* | *day month*} [*year*]] | **in** {**hour** *hours* | **minute** *minutes* | **hour** *hours* **minute** *minutes*} | **regularity** *hour minute* [**period** {**daily** | **weekly** *day-of-week* | **monthly** *day*}] | **cancel** [**at** | **in** | **regularity**]}

reload at - A specified time at which to reload the switch.

hour - The hour at which to reload. (Range: 0-23)

minute - The minute at which to reload. (Range: 0-59)

month - The month at which to reload. (january ... december)

day - The day of the month at which to reload. (Range: 1-31)

year - The year at which to reload. (Range: 2001-2050)

reload in - An interval after which to reload the switch.

hours - The number of hours, combined with the minutes, before the switch resets. (Range: 0-576)

minutes - The number of minutes, combined with the hours, before the switch resets. (Range: 0-59)

reload regularity - A periodic interval at which to reload the switch.

hour - The hour at which to reload. (Range: 0-23)

minute - The minute at which to reload. (Range: 0-59)

day-of-week - Day of the week at which to reload. (Range: monday ... saturday)

day - Day of the month at which to reload. (Range: 1-31)

reload cancel - Cancels the specified reload option.

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command resets the entire system.
- Any combination of reload options may be specified. If the same option is re-specified, the previous setting will be overwritten.
- When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory by the copy running-config startup-config command (See the copy command).

EXAMPLE

This example shows how to reset the switch after 30 minutes:

```
Console(config)#reload in minute 30
***
*** --- Rebooting at January  1 02:10:43 2007 ---
***

Are you sure to reboot the system at the specified time? <y/n>
```

enable

This command activates Privileged Exec mode. In privileged mode, additional commands are available, and certain commands display additional information. See "Understanding Command Modes."

SYNTAX

enable [*level*]

level - Privilege level to log into the device.

The device has two predefined privilege levels: 0: Normal Exec, 15: Privileged Exec. Enter level 15 to access Privileged Exec mode.

DEFAULT SETTING

Level 15

COMMAND MODE

Normal Exec

COMMAND USAGE

- "super" is the default password required to change the command mode from Normal Exec to Privileged Exec. (To set this password, see the enable password command.)
- The "#" character is appended to the end of the prompt to indicate that the system is in privileged access mode.

EXAMPLE

```
Console>enable
Password: [privileged level password]
Console#
```

RELATED COMMANDS

disable (450)
enable password (554)

quit

This command exits the configuration program.

DEFAULT SETTING

None

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

The **quit** and **exit** commands can both exit the configuration program.

EXAMPLE

This example shows how to quit a CLI session:

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```

show history

This command shows the contents of the command history buffer.

DEFAULT SETTING

None

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

The history buffer size is fixed at 10 Execution commands and 10 Configuration commands.

EXAMPLE

In this example, the show history command lists the contents of the command history buffer:

```
Console#show history
Execution command history:
 2 config
 1 show history

Configuration command history:
 4 interface vlan 1
 3 exit
 2 interface vlan 1
 1 end

Console#
```

The **!** command repeats commands from the Execution command history buffer when you are in Normal Exec or Privileged Exec Mode, and commands from the Configuration command history buffer when you are in any of the configuration modes. In this example, the **!2** command repeats the second command in the Execution history buffer (**config**).

```
Console#!2
Console#config
Console(config)#
```

configure

This command activates Global Configuration mode. You must enter this mode to modify any settings on the switch. You must also enter Global Configuration mode prior to enabling some of the other configuration modes, such as Interface Configuration, Line Configuration, and VLAN Database Configuration. See "Understanding Command Modes."

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#configure
Console(config)#
```

RELATED COMMANDS

end (451)

disable

This command returns to Normal Exec mode from privileged mode. In normal access mode, you can only display basic information on the switch's configuration or Ethernet statistics. To gain access to all commands, you must use the privileged mode. See "Understanding Command Modes."

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

The ">" character is appended to the end of the prompt to indicate that the system is in normal access mode.

EXAMPLE

```
Console#disable
Console>
```

RELATED COMMANDS

enable (447)

reload (Privileged Exec)

This command restarts the system.

NOTE: When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory by the copy running-config startup-config command.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

This command resets the entire system.

EXAMPLE

This example shows how to reset the switch:

```
Console#reload
Note: It takes around 100~120 seconds to finish system reboot.
Do you really want to reset the switch?
```

show reload

This command displays the current reload settings, and the time at which next scheduled reload will take place.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show reload
Reloading switch in time:                        0 hours 29 minutes.

The switch will be rebooted at January  1 02:11:50 2001.
Remaining Time: 0 days, 0 hours, 29 minutes, 52 seconds.
Console#
```

end

This command returns to Privileged Exec mode.

DEFAULT SETTING

None

COMMAND MODE

Global Configuration, Interface Configuration, Line Configuration, VLAN Database Configuration, and Multiple Spanning Tree Configuration.

EXAMPLE

This example shows how to return to the Privileged Exec mode from the Interface Configuration mode:

```
Console(config-if)#end
Console#
```

exit

This command returns to the previous configuration mode or exits the configuration program.

DEFAULT SETTING

None

COMMAND MODE

Any

EXAMPLE

This example shows how to return to the Privileged Exec mode from the Global Configuration mode, and then quit the CLI session:

```
Console(config)#exit
Console#exit

Press ENTER to start session

User Access Verification

Username:
```

21 SYSTEM MANAGEMENT COMMANDS

These commands are used to control system logs, passwords, user names, management options, and display or configure a variety of other system information.

Table 36: System Management Commands

Command Group	Function
Device Designation	Configures information that uniquely identifies this switch
Banner Information	Configures administrative contact, device identification and location
System Status	Displays system configuration, active managers, and version information
Frame Size	Enables support for jumbo frames
File Management	Manages code image or switch configuration files
Line	Sets communication parameters for the serial port, including baud rate and console time-out
Event Logging	Controls logging of error messages
SMTP Alerts	Configures SMTP email alerts
Time (System Clock)	Sets the system clock automatically via NTP/SNTP server or manually
Time Range	Sets a time range for use by other functions, such as Access Control Lists
Switch Clustering	Configures management of multiple devices via a single IP address
UPnP	Sets Universal Plug-and-Play parameters used to advertise the switch

DEVICE DESIGNATION

This section describes commands used to configure information that uniquely identifies the switch.

Table 37: Device Designation Commands

Command	Function	Mode
hostname	Specifies the host name for the switch	GC
snmp-server contact	Sets the system contact string	GC
snmp-server location	Sets the system location string	GC

hostname

This command specifies or modifies the host name for this device. Use the **no** form to restore the default host name.

SYNTAX

hostname *name*

no hostname

name - The name of this host. (Maximum length: 255 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#hostname RD#1
Console(config)#
```

BANNER INFORMATION

These commands are used to configure and manage administrative information about the switch, its exact data center location, details of the electrical and network circuits that supply the switch, as well as contact information for the network administrator and system manager. This information is only available via the CLI and is automatically displayed before login as soon as a console or telnet connection has been established.

Table 38: Banner Commands

Command	Function	Mode
banner configure	Configures the banner information that is displayed before login	GC
banner configure company	Configures the Company information that is displayed by banner	GC
banner configure dc-power-info	Configures the DC Power information that is displayed by banner	GC
banner configure department	Configures the Department information that is displayed by banner	GC
banner configure equipment-info	Configures the Equipment information that is displayed by banner	GC
banner configure equipment-location	Configures the Equipment Location information that is displayed by banner	GC
banner configure ip-lan	Configures the IP and LAN information that is displayed by banner	GC
banner configure lp-number	Configures the LP Number information that is displayed by banner	GC

Table 38: Banner Commands (Continued)

Command	Function	Mode
banner configure manager-info	Configures the Manager contact information that is displayed by banner	GC
banner configure mux	Configures the MUX information that is displayed by banner	GC
banner configure note	Configures miscellaneous information that is displayed by banner under the Notes heading	GC
show banner	Displays all banner information	NE, PE

banner configure

This command is used to interactively specify administrative information for this device.

SYNTAX

banner configure

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

The administrator can batch-input all details for the switch with one command. When the administrator finishes typing the company name and presses the enter key, the script prompts for the next piece of information, and so on, until all information has been entered. Pressing enter without inputting information at any prompt during the script's operation will leave the field empty. Spaces can be used during script mode because pressing the enter key signifies the end of data input. The delete and left-arrow keys terminate the script. The use of the backspace key during script mode is not supported. If, for example, a mistake is made in the company name, it can be corrected with the **banner configure company** command.

EXAMPLE

```
Console(config)#banner configure

Company: EdgeCore Networks
Responsible department: R&D Dept
Name and telephone to Contact the management people
Manager1 name: Sr. Network Admin
 phone number: 123-555-1212
Manager2 name: Jr. Network Admin
 phone number: 123-555-1213
Manager3 name: Night-shift Net Admin / Janitor
 phone number: 123-555-1214
The physical location of the equipment.
City and street address: 12 Straight St. Motown, Zimbabwe
Information about this equipment:
Manufacturer: EdgeCore Networks
ID: 123_unique_id_number
Floor: 2
```

```
Row: 7
Rack: 29
Shelf in this rack: 8
Information about DC power supply.
Floor: 2
Row: 7
Rack: 25
Electrical circuit: : ec-177743209-xb
Number of LP:12
Position of the equipment in the MUX:1/23
IP LAN:192.168.1.1
Note: This is a random note about this managed switch and can contain
  miscellaneous information.
Console(config)#
```

banner configure company

This command is used to configure company information displayed in the banner. Use the **no** form to remove the company name from the banner display.

SYNTAX

banner configure company *name*

no banner configure company

name - The name of the company. (Maximum length: 32 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

Input strings cannot contain spaces. The **banner configure company** command interprets spaces as data input boundaries. The use of underscores (_) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure company LG-Nortel
Console(config)#
```

banner configure dc-power-info

This command is use to configure DC power information displayed in the banner. Use the **no** form to restore the default setting.

SYNTAX

banner configure dc-power-info floor *floor-id* **row** *row-id* **rack** *rack-id* **electrical-circuit** *ec-id*

no banner configure dc-power-info [**floor** | **row** | **rack** | **electrical-circuit**]

floor-id - The floor number.

row-id - The row number.

rack-id - The rack number.

ec-id - The electrical circuit ID.

Maximum length of each parameter: 32 characters

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

Input strings cannot contain spaces. The **banner configure dc-power-info** command interprets spaces as data input boundaries. The use of underscores (_) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure dc-power-info floor 3 row 15 rack 24
  electrical-circuit 48v-id_3.15.24.2
Console(config)#
```

banner configure department

This command is used to configure the department information displayed in the banner. Use the **no** form to restore the default setting.

SYNTAX

banner configure department *dept-name*

no banner configure company

dept-name - The name of the department. (Maximum length: 32 characters)

DEFAULT SETTING

None

COMMAND MODE
Global Configuration

COMMAND USAGE
Input strings cannot contain spaces. The **banner configure department** command interprets spaces as data input boundaries. The use of underscores (_) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure department R&D
Console(config)#
```

banner configure equipment-info

This command is used to configure the equipment information displayed in the banner. Use the **no** form to restore the default setting.

SYNTAX

banner configure equipment-info manufacturer-id *mfr-id* **floor** *floor-id* **row** *row-id* **rack** *rack-id* **shelf-rack** *sr-id* **manufacturer** *mfr-name*

no banner configure equipment-info [**floor** | **manufacturer** | **manufacturer-id** | **rack** | **row** | **shelf-rack**]

mfr-id - The name of the device model number.

floor-id - The floor number.

row-id - The row number.

rack-id - The rack number.

sr-id - The shelf number in the rack.

mfr-name - The name of the device manufacturer.

Maximum length of each parameter: 32 characters

DEFAULT SETTING
None

COMMAND MODE
Global Configuration

COMMAND USAGE
Input strings cannot contain spaces. The **banner configure equipment-info** command interprets spaces as data input boundaries. The use of underscores (_) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure equipment-info manufacturer-id ES3510MA
  floor 3 row 10 rack 15 shelf-rack 12 manufacturer EdgeCore
Console(config)#
```

banner configure equipment-location

This command is used to configure the equipment location information displayed in the banner. Use the **no** form to restore the default setting.

SYNTAX

banner configure equipment-location *location*

no banner configure equipment-location

location - The address location of the device. (Maximum length: 32 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

Input strings cannot contain spaces. The **banner configure equipment-location** command interprets spaces as data input boundaries. The use of underscores (_) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure equipment-location
  710_Network_Path,_Indianapolis
Console(config)#
```

banner configure ip-lan

This command is used to configure the device IP address and subnet mask information displayed in the banner. Use the **no** form to restore the default setting.

SYNTAX

banner configure ip-lan *ip-mask*

no banner configure ip-lan

ip-mask - The IP address and subnet mask of the device. (Maximum length: 32 characters)

DEFAULT SETTING

None

COMMAND MODE
Global Configuration

COMMAND USAGE
Input strings cannot contain spaces. The **banner configure ip-lan** command interprets spaces as data input boundaries. The use of underscores (_) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure ip-lan 192.168.1.1/255.255.255.0
Console(config)#
```

banner configure lp-number

This command is used to configure the LP number information displayed in the banner. Use the **no** form to restore the default setting.

SYNTAX

banner configure lp-number *lp-num*

no banner configure lp-number

lp-num - The LP number. (Maximum length: 32 characters)

DEFAULT SETTING
None

COMMAND MODE
Global Configuration

COMMAND USAGE
Input strings cannot contain spaces. The **banner configure lp-number** command interprets spaces as data input boundaries. The use of underscores (_) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure lp-number 12
Console(config)#
```

banner configure manager-info

This command is used to configure the manager contact information displayed in the banner. Use the **no** form to restore the default setting.

SYNTAX

banner configure manager-info
name *mgr1-name* **phone-number** *mgr1-number*
[**name2** *mgr2-name* **phone-number** *mgr2-number* |
name3 *mgr3-name* **phone-number** *mgr3-number*]

no banner configure manager-info [**name1** | **name2** | **name3**]

mgr1-name - The name of the first manager.

mgr1-number - The phone number of the first manager.

mgr2-name - The name of the second manager.

mgr2-number - The phone number of the second manager.

mgr3-name - The name of the third manager.

mgr3-number - The phone number of the third manager.

Maximum length of each parameter: 32 characters

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

Input strings cannot contain spaces. The **banner configure manager-info** command interprets spaces as data input boundaries. The use of underscores (_) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure manager-info name Albert_Einstein phone-
  number 123-555-1212 name2 Lamar phone-number 123-555-1219
Console(config)#
```

banner configure mux

This command is used to configure the mux information displayed in the banner. Use the **no** form to restore the default setting.

SYNTAX

banner configure mux *muxinfo*

no banner configure mux

muxinfo - The circuit and PVC to which the switch is connected. (Maximum length: 32 characters)

DEFAULT SETTING
None

COMMAND MODE
Global Configuration

COMMAND USAGE
Input strings cannot contain spaces. The **banner configure mux** command interprets spaces as data input boundaries. The use of underscores (_) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure mux telco-8734212kx_PVC-1/23
Console(config)#
```

banner configure note

This command is used to configure the note displayed in the banner. Use the **no** form to restore the default setting.

SYNTAX

banner configure note *note-info*

no banner configure note

note-info - Miscellaneous information that does not fit the other banner categories, or any other information of importance to users of the switch CLI. (Maximum length: 150 characters)

DEFAULT SETTING
None

COMMAND MODE
Global Configuration

COMMAND USAGE
Input strings cannot contain spaces. The **banner configure note** command interprets spaces as data input boundaries. The use of underscores (_) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure note !!!!!ROUTINE_MAINTENANCE_firmware-
  upgrade_0100-0500_GMT-0500_20071022!!!!!_20min_network_impact_expected
Console(config)#
```

show banner

This command displays all banner information.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
Console#show banner
EdgeCore
WARNING - MONITORED ACTIONS AND ACCESSES
R&D

Albert_Einstein - 123-555-1212
Lamar - 123-555-1219

Station's information:
710_Network_Path,_Indianapolis

 EdgeCore- ES3510MA
Floor / Row / Rack / Sub-Rack
 3/ 10 / 15 / 12
DC power supply:
Power Source A: Floor / Row / Rack / Electrical circuit
 3/ 15 / 24 / 48v-id_3.15.24.2
Number of LP: 12
Position MUX: telco-8734212kx_PVC-1/23
IP LAN: 192.168.1.1/255.255.255.0
Note: !!!!!ROUTINE_MAINTENANCE_firmware-upgrade_0100-0500_GMT-
  0500_20071022!!!!!_20min_network_
Console#
```

SYSTEM STATUS

This section describes commands used to display system information.

Table 39: System Status Commands

Command	Function	Mode
show access-list tcam-utilization	Shows utilization parameters for TCAM	PE
show memory	Shows memory utilization parameters	NE, PE
show process cpu	Shows CPU utilization parameters	NE, PE
show running-config	Displays the configuration data currently in use	PE
show startup-config	Displays the contents of the configuration file (stored in flash memory) that is used to start up the system	PE
show system	Displays system information	NE, PE
show tech-support	Displays a detailed list of system settings designed to help technical support resolve configuration or functional problems	PE
show users	Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet clients	NE, PE
show version	Displays version information for the system	NE, PE

show access-list tcam-utilization

This command shows utilization parameters for TCAM (Ternary Content Addressable Memory), including the number policy control entries in use, the number of free entries, and the overall percentage of TCAM in use.

COMMAND MODE

Privileged Exec

COMMAND USAGE

Policy control entries (PCEs) are used by various system functions which rely on rule-based searches, including Access Control Lists (ACLs), IP Source Guard filter rules, Quality of Service (QoS) processes, or traps.

For example, when binding an ACL to a port, each rule in an ACL will use two PCEs; and when setting an IP Source Guard filter rule for a port, the system will also use two PCEs.

EXAMPLE

```
Console#show access-list tcam-utilization
  Total Policy Control Entries    : 512
  Free Policy Control Entries     : 352
  TCAM Utilization                : 31.25%
Console#
```

show memory

This command shows memory utilization parameters.

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

This command shows the amount of memory currently free for use, and the amount of memory allocated to active processes.

EXAMPLE

```
Console#show memory
 Status   Bytes      Blocks   Avg Block Size Max Block Size
 ------ ---------- ---------- -------------- --------------
 Free     12692856          40         317321       12304432
 Alloc    11933416       51323            232              -

Console#
```

show process cpu

This command shows the CPU utilization parameters.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
Console#show process cpu
 CPU Utilization in the past 5 seconds : 3.98%
Console#
```

show running-config

This command displays the configuration information currently in use.

SYNTAX

show running-config *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

vlan *vlan-id* (Range: 1-4093)

COMMAND MODE

Privileged Exec

COMMAND USAGE

- Use this command in conjunction with the **show startup-config** command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by "!" symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
  - MAC address for the switch
  - SNTP server settings
  - SNMP community strings
  - Users (names, access levels, and encrypted passwords)
  - VLAN database (VLAN ID, name and state)
  - VLAN configuration settings for each interface
  - Multiple spanning tree instances (name and interfaces)
  - IP address configured for management VLAN
  - Spanning tree settings
  - Interface settings
  - Any configured settings for the console port and Telnet
- When the system pauses after displaying the first page, press "a" to force the system to display the rest of the configuration settings without pausing.

EXAMPLE

```
Console#show running-config
Building startup configuration. Please wait...
!<stackingDB>00</stackingDB>
!<stackingMac>01_00-e0-0c-00-00-fd_00</stackingMac>
!
sntp server 0.0.0.0 0.0.0.0 0.0.0.0
!
no dot1q-tunnel system-tunnel-control
!
snmp-server community public ro
snmp-server community private rw
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
 VLAN 1 name DefaultVlan media ethernet state active
 no vlan 4093
!
spanning-tree mst configuration
!
interface vlan 1
 ip address dhcp
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
⋮

!
line console
 silent-time 0
!
line VTY
!
end
!
Console#
```

RELATED COMMANDS

show startup-config (466)

show startup-config

This command displays the configuration file stored in non-volatile memory that is used to start up the system.

COMMAND MODE

Privileged Exec

COMMAND USAGE

- Use this command in conjunction with the **show running-config** command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by "!" symbols, and includes the configuration mode

command, and corresponding commands. This command displays the following information:

- MAC address for the switch
- SNTP server settings
- SNMP community strings
- Users (names, access levels, and encrypted passwords)
- VLAN database (VLAN ID, name and state)
- VLAN configuration settings for each interface
- Multiple spanning tree instances (name and interfaces)
- IP address configured for management VLAN
- Spanning tree settings
- Interface settings
- Any configured settings for the console port and Telnet

EXAMPLE

Refer to the example for the running configuration file.

RELATED COMMANDS

show running-config (465)

show system

This command displays system information.

DEFAULT SETTING

None

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

- For a description of the items shown by this command, refer to "Displaying System Information."
- The POST results should all display "PASS." If any POST test indicates "FAIL," contact your distributor for assistance.

EXAMPLE

```
Console#show system
System Description: Edge-Core FE L2 Switch ES3528M
System OID String: 1.3.6.1.4.1.259.6.10.94
System Information
 System Up Time:          0 days, 0 hours, 5 minutes, and 41.90 seconds
 System Name:             [NONE]
 System Location:         [NONE]
 System Contact:          [NONE]
 MAC Address (Unit1):     00-12-CF-61-24-2F
 Web Server:              Enabled
 Web Server Port:         80
 Web Secure Server:       Enabled
 Web Secure Server Port:  443
 Telnet Server:           Enable
 Telnet Server Port:      23
 Jumbo Frame:             Disabled
```

```
Timer Test ..................... PASS
UART Loopback Test ............. PASS
DRAM Test ...................... PASS
Switch Int Loopback Test ..... PASS

Console#
```

show tech-support

This command displays a detailed list of system settings designed to help technical support resolve configuration or functional problems.

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

This command generates a long list of information including detailed system and interface settings. It is therefore advisable to direct the output to a file using any suitable output capture function provided with your terminal emulation program.

EXAMPLE

```
Console#show tech-support

show system:
System Description: Edge-Core FE L2 Switch ES3528M
System OID String: 1.3.6.1.4.1.259.6.10.94
System Information
 System Up Time:          0 days, 2 hours, 17 minutes, and 6.23 seconds
 System Name:             [NONE]
 System Location:         [NONE]
 System Contact:          [NONE]
 MAC Address (Unit1):     00-12-CF-61-24-2F
 Web Server:              Enabled
 Web Server Port:         80
 Web Secure Server:       Enabled
 Web Secure Server Port:  443
 Telnet Server:           Enable
 Telnet Server Port:      23
 Jumbo Frame:             Disabled
:
```

show users

Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet client.

DEFAULT SETTING

None

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

The session used to execute this command is indicated by a "*" symbol next to the Line (i.e., session) index number.

EXAMPLE

```
Console#show users
 User Name Accounts:
  User Name Privilege Public-Key
  --------- --------- ----------
      admin        15 None
      guest         0 None
      steve        15  RSA

 Online Users:
  Line        Username Idle time (h:m:s) Remote IP addr.
  ----------- -------- ----------------- ---------------
  0   console    admin           0:14:14
* 1     VTY 0    admin           0:00:00    192.168.1.19
  2     SSH 1    steve           0:00:06    192.168.1.19

 Web Online Users:
  Line        Remote IP Addr  User Name Idle time (h:m:s)
  ----------- --------------- --------- ------------------
  1      HTTP    192.168.1.19     admin            0:00:00

Console#
```

show version

This command displays hardware and software version information for the system.

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

See "Displaying Switch Hardware/Software Versions" for detailed information on the items displayed by this command.

EXAMPLE

```
Console#show version
Unit 1
 Serial Number:           A733006612
 Hardware Version:        R01
 Chip Device ID:          Marvell 98DX107-A2, 88E6095[F]
 EPLD Version:            0.07
 Number of Ports:         28
 Main Power Status:       Up
 Redundant Power Status:  Not present

Agent (Master)
 Unit ID:                 1
 Loader Version:          1.0.2.0
 Boot ROM Version:        1.2.0.1
 Operation Code Version:  1.4.6.1

Console#
```

FRAME SIZE

This section describes commands used to configure the Ethernet frame size on the switch.

Table 40: Frame Size Commands

Command	Function	Mode
jumbo frame	Enables support for jumbo frames	GC

jumbo frame

This command enables support for jumbo frames for Gigabit Ethernet ports. Use the **no** form to disable it.

SYNTAX

[**no**] **jumbo frame**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- This switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames on Gigabit Ethernet ports up to 10 KB. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.
- To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.
- The current setting for jumbo frames can be displayed with the show system command.

EXAMPLE

```
Console(config)#jumbo frame
Console(config)#
```

FILE MANAGEMENT

Managing Firmware

Firmware can be uploaded and downloaded to or from an FTP/TFTP server. By saving runtime code to a file on an FTP/TFTP server, that file can later be downloaded to the switch to restore operation. The switch can also be set to use new firmware without overwriting the previous version.

When downloading runtime code, the destination file name can be specified to replace the current image, or the file can be first downloaded using a different name from the current runtime code file, and then the new file set as the startup file.

Saving or Restoring Configuration Settings

Configuration settings can be uploaded and downloaded to and from an FTP/TFTP server. The configuration file can be later downloaded to restore switch settings.

The configuration file can be downloaded under a new file name and then set as the startup file, or the current startup configuration file can be specified as the destination file to directly replace it. Note that the file "Factory_Default_Config.cfg" can be copied to the FTP/TFTP server, but cannot be used as the destination on the switch.

Table 41: Flash/File Commands

Command	Function	Mode
boot system	Specifies the file or image used to start up the system	GC
copy	Copies a code image or a switch configuration to or from flash memory or an FTP/TFTP server	PE
delete	Deletes a configuration file or code image	PE
delete non-active	Deletes all configuration files or code images not set as startup files	PE
dir	Displays a list of files in flash memory	PE
whichboot	Displays the files booted	PE
Automatic Code Upgrade Commands		
upgrade opcode auto	Automatically upgrades the current image when a new version is detected on the indicated server	GC
upgrade opcode path	Specifies an FTP/TFTP server and directory in which the new opcode is stored	GC
show upgrade	Shows if automatic upgrade is enabled, the upgrade path, and the name of the opcode.	PE

boot system

This command specifies the file or image used to start up the system.

SYNTAX

boot system {**boot-rom** | **config** | **opcode**}: *filename*

boot-rom* - Boot ROM.

config* - Configuration file.

opcode* - Run-time operation code.

filename - Name of configuration file or code image.

* The colon (:) is required.

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- A colon (:) is required after the specified file type.
- If the file contains an error, it cannot be set as the default file.

EXAMPLE

```
Console(config)#boot system config: startup
Console(config)#
```

RELATED COMMANDS

dir (477)
whichboot (478)

copy

This command moves (upload/download) a code image or configuration file between the switch's flash memory and an FTP/TFTP server. When you save the system code or configuration settings to a file on an FTP/TFTP server, that file can later be downloaded to the switch to restore system operation. The success of the file transfer depends on the accessibility of the TFTP server and the quality of the network connection.

SYNTAX

copy file {**file** | **ftp** | **running-config** | **startup-config** | **tftp**}
copy running-config {**file** | **ftp** | **startup-config** | **tftp**}
copy startup-config {**file** | **ftp** | **running-config** | **tftp**}
copy tftp {**add-to-running-config** | **file** | **https-certificate** | **public-key** | **running-config** | **startup-config**}

add-to-running-config - Keyword that adds the settings listed in the specified file to the running configuration.

file - Keyword that allows you to copy to/from a file.

ftp - Keyword that allows you to copy to/from an FTP server.

https-certificate - Keyword that allows you to copy the HTTPS secure site certificate.

public-key - Keyword that allows you to copy a SSH key from a TFTP server. (See "Secure Shell.")

running-config - Keyword that allows you to copy to/from the current running configuration.

startup-config - The configuration used for system initialization.

tftp - Keyword that allows you to copy to/from a TFTP server.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

- The system prompts for data required to complete the copy command.
- The destination file name should not contain slashes (\ or /), and the maximum length for file names is 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-")
- The switch supports only two operation code files, but the maximum number of user-defined configuration files is 16.
- You can use "Factory_Default_Config.cfg" as the source to copy from the factory default configuration file, but you cannot use it as the destination.
- To replace the startup configuration, you must use **startup-config** as the destination.

- The Boot ROM and Loader can be downloaded from an FTP/TFTP server, but cannot be uploaded from the switch to a file server.
- For information on specifying an https-certificate, see "Replacing the Default Secure-site Certificate." For information on configuring the switch to use HTTPS for a secure connection, see the ip http secure-server command.
- When logging into an FTP server, the interface prompts for a user name and password configured on the remote server. Note that "anonymous" is set as the default user name.

EXAMPLE

The following example shows how to download new firmware from a TFTP server:

```
Console#copy tftp file
TFTP server ip address: 10.1.0.19
Choose file type:
1. config; 2. opcode; 4. diag; 5. loader: 2
Source file name: m360.bix
Destination file name: m360.bix
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#
```

The following example shows how to upload the configuration settings to a file on the TFTP server:

```
Console#copy file tftp
Choose file type:
 1. config:  2. opcode: <1-2>: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
TFTP completed.
Success.

Console#
```

The following example shows how to copy the running configuration to a startup file.

```
Console#copy running-config file
Destination configuration file name: startup
Write to FLASH Programming.
\Write to FLASH finish.
Success.

Console#
```

The following example shows how to download a configuration file:

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
Write to FLASH Programming.

\Write to FLASH finish.
Success.

Console#
```

This example shows how to copy a secure-site certificate from an TFTP server. It then reboots the switch to activate the certificate:

```
Console#copy tftp https-certificate
TFTP server ip address: 10.1.0.19
Source certificate file name: SS-certificate
Source private file name: SS-private
Private password: ********

Success.
Console#reload
System will be restarted, continue <y/n>? y
```

This example shows how to copy a public-key used by SSH from an TFTP server. Note that public key authentication via SSH is only supported for users configured locally on the switch.

```
Console#copy tftp public-key
TFTP server IP address: 192.168.1.19
Choose public key type:
 1. RSA; 2. DSA: 1
Source file name: steve.pub
Username: steve
TFTP Download
Success.
Write to FLASH Programming.
Success.

Console#
```

This example shows how to copy a file to an FTP server.

```
Console#copy ftp file
FTP server IP address: 169.254.1.11
User[Anonymous]: admin
Password[]: *****
Choose file type:
1. config; 2. opcode; 4. diag; 5. loader: 2
Source file name: BLANC.BIX
Destination file name: BLANC.BIX
Console#
```

delete

This command deletes a file or image.

SYNTAX

delete *filename*

filename - Name of configuration file or code image.

COMMAND MODE

Privileged Exec

COMMAND USAGE

- If the file type is used for system startup, then this file cannot be deleted.
- "Factory_Default_Config.cfg" cannot be deleted.

EXAMPLE

This example shows how to delete the test2.cfg configuration file from flash memory.

```
Console#delete test2.cfg
Console#
```

RELATED COMMANDS

dir (477)
delete public-key (586)

delete non-active

This command deletes all configuration or operation code files which are not set as startup files.

SYNTAX

delete non-active [**config** | **opcode**]

config - Switch configuration file.

opcode - Run-time operation code image file.

COMMAND MODE

Privileged Exec

COMMAND USAGE

- If neither the **config** nor **opcode** keyword is specified, all configuration and operation code files not set as startup files are deleted.
- "Factory_Default_Config.cfg" cannot be deleted.

EXAMPLE

This example deletes all non-startup files.

```
Console#delete non-active
Are you sure to delete non-active file(s)? [Y]es/[N]o:

 Unit 1:
      Success to delete [ES3528_52M_op_V1.4.2.1.bix]
      Factory Default Configuration file couldn't be deleted.
Console#
```

RELATED COMMANDS

dir (477)
delete public-key (586)

dir

This command displays a list of files in flash memory.

SYNTAX

dir {**boot-rom:** | **config:** | **opcode:**} [*filename*]}

boot-rom - Boot ROM (or diagnostic) image file.

config - Switch configuration file.

opcode - Run-time operation code image file.

filename - Name of configuration file or code image. If this file exists but contains errors, information on this file cannot be shown.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

- If you enter the command **dir** without any parameters, the system displays all files.

  File information is shown below:

Table 42: File Directory Information

Column Heading	Description
File Name	The name of the file.
File Type	File types: Boot-Rom, Operation Code, and Config file.
Startup	Shows if this file is used when the system is started.
Size	The length of the file in bytes.

EXAMPLE

The following example shows how to display all file information:

```
Console#dir
          File name                          File type       Startup Size (byte)
 ------------------------------------     --------------  ------- -----------
 Unit1:
          ES3528_52M_diag_V1.2.0.1.bix     Boot-Rom Image  Y          1406420
          ES3528_52M_opcode_V1.4.4.0.bix   Operation Code  N          4706820
          ES3528_52M_opcode_V1.4.6.1.bix   Operation Code  Y          4791940
          Factory_Default_Config.cfg       Config File     N              455
          startup1.cfg                     Config File     Y             2708
 ------------------------------------------------------------------------------
                                                  Total free space:   4325376
Console#
```

whichboot

This command displays which files were booted when the system powered up.

SYNTAX

whichboot

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

This example shows the information displayed by the **whichboot** command. See the table under the **dir** command for a description of the file information displayed by this command.

```
Console#whichboot
          File name                           File type      Startup  Size (byte)
 ---------------------------------------  --------------  -------  -----------
 Unit1:
          ES3528_52M_diag_V1.2.0.1.bix     Boot-Rom Image  Y          1406420
          ES3528_52M_opcode_V1.4.6.1.bix   Operation Code  Y          4791940
          startup1.cfg                     Config File     Y             2708

Console#
```

upgrade opcode auto

This command automatically upgrades the current operational code when a new version is detected on the server indicated by the upgrade opcode path command. Use the **no** form of this command to restore the default setting.

SYNTAX

[**no**] **upgrade opcode auto**

DEFAULT SETTING
Disabled

COMMAND MODE
Global Configuration

COMMAND USAGE
- This command is used to enable or disable automatic upgrade of the operational code. When the switch starts up and automatic image upgrade is enabled by this command, the switch will follow these steps when it boots up:

  1. It will search for a new version of the image at the location specified by upgrade opcode path command. The name for the new image stored on the TFTP server must be ES3552M-PoE.bix. If the switch detects a code version newer than the one currently in use, it will download the new image. If two code images are already stored in the switch, the image not set to start up the system will be overwritten by the new version.

  2. After the image has been downloaded, the switch will send a trap message to log whether or not the upgrade operation was successful.

  3. It sets the new version as the startup image.

  4. It then restarts the system to start using the new image.

- Any changes made to the default setting can be displayed with the show running-config or show startup-config commands.

EXAMPLE
```
Console(config)#upgrade opcode auto
Console(config)#upgrade opcode path tftp://192.168.0.1/sm24/
Console(config)#
```

If a new image is found at the specified location, the following type of messages will be displayed during bootup.

```
⋮
Automatic Upgrade is looking for a new image
New image detected: current version 1.1.1.0; new version 1.1.1.2
Image upgrade in progress
The switch will restart after upgrade succeeds
Downloading new image
Flash programming started
Flash programming completed
The switch will now restart
⋮
```

upgrade opcode path

This command specifies an TFTP server and directory in which the new opcode is stored. Use the **no** form of this command to clear the current setting.

SYNTAX

upgrade opcode path *opcode-dir-url*

no upgrade opcode path

opcode-dir-url - The location of the new code.

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command is used in conjunction with the upgrade opcode auto command to facilitate automatic upgrade of new operational code stored at the location indicated by this command.
- The name for the new image stored on the TFTP server must be es3510ma.bix. However, note that file name is not to be included in this command.
- When specifying a TFTP server, the following syntax must be used, where *filedir* indicates the path to the directory containing the new image:

  ```
  tftp://192.168.0.1[/filedir]/
  ```

- When specifying an FTP server, the following syntax must be used, where *filedir* indicates the path to the directory containing the new image:

  ```
  ftp://[username[:password@]]192.168.0.1[/filedir]/
  ```

  If the user name is omitted, "Anonymous" will be used for the connection. If the password is omitted a null string ("") will be used for the connection.

EXAMPLE

This shows how to specify a TFTP server where new code is stored.

```
Console(config)#upgrade opcode path tftp://192.168.0.1/sm24/
Console(config)#
```

This shows how to specify an FTP server where new code is stored.

```
Console(config)#upgrade opcode path ftp://admin:billy@192.168.0.1/sm24/
Console(config)#
```

show upgrade

This command shows if automatic opcode upgrade is enabled, the upgrade path on the file server, and the name of the opcode.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show upgrade
  Status : Enabled
  Path   : tftp://192.168.0.1/SM24/
  File Name : ES3552M-PoE.bix
Console#
```

LINE

You can access the onboard configuration program by attaching a VT100 compatible device to the server's serial port. These commands are used to set communication parameters for the serial port or Telnet (i.e., a virtual terminal).

Table 43: Line Commands

Command	Function	Mode
line	Identifies a specific line for configuration and starts the line configuration mode	GC
accounting commands	Applies an accounting method to CLI commands entered by a user	LC
accounting exec	Applies an accounting method to local console, Telnet or SSH connections	LC
authorization exec	Applies an authorization method to local console, Telnet or SSH connections	LC
databits*	Sets the number of data bits per character that are interpreted and generated by hardware	LC
exec-timeout	Sets the interval that the command interpreter waits until user input is detected	LC
login	Enables password checking at login	LC
parity*	Defines the generation of a parity bit	LC
password	Specifies a password on a line	LC
password-thresh	Sets the password intrusion threshold, which limits the number of failed logon attempts	LC
silent-time*	Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the password-thresh command	LC
speed*	Sets the terminal baud rate	LC
stopbits*	Sets the number of the stop bits transmitted per byte	LC
timeout login response	Sets the interval that the system waits for a login attempt	LC

Table 43: Line Commands (Continued)

Command	Function	Mode
disconnect	Terminates a line connection	PE
show line	Displays a terminal line's parameters	NE, PE

* These commands only apply to the serial port.

line

This command identifies a specific line for configuration, and to process subsequent line configuration commands.

SYNTAX

line {**console** | **vty**}

console - Console terminal line.

vty - Virtual terminal for remote console access (i.e., Telnet).

DEFAULT SETTING

There is no default line.

COMMAND MODE

Global Configuration

COMMAND USAGE

Telnet is considered a virtual terminal connection and will be shown as "VTY" in screen displays such as show users. However, the serial communication parameters (e.g., databits) do not affect Telnet connections.

EXAMPLE

To enter console line mode, enter the following command:

```
Console(config)#line console
Console(config-line)#
```

RELATED COMMANDS

show line (490)
show users (468)

databits

This command sets the number of data bits per character that are interpreted and generated by the console port. Use the **no** form to restore the default value.

SYNTAX

databits {**7** | **8**}

no databits

7 - Seven data bits per character.

8 - Eight data bits per character.

DEFAULT SETTING

8 data bits per character

COMMAND MODE

Line Configuration

COMMAND USAGE

The **databits** command can be used to mask the high bit on input from devices that generate 7 data bits with parity. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character.

EXAMPLE

To specify 7 data bits, enter this command:

```
Console(config-line)#databits 7
Console(config-line)#
```

RELATED COMMANDS

parity (485)

exec-timeout

This command sets the interval that the system waits until user input is detected. Use the **no** form to restore the default.

SYNTAX

exec-timeout [*seconds*]

no exec-timeout

seconds - Integer that specifies the timeout interval. (Range: 0 - 65535 seconds; 0: no timeout)

DEFAULT SETTING

CLI: No timeout
Telnet: 10 minutes

COMMAND MODE

Line Configuration

COMMAND USAGE

- If user input is detected within the timeout interval, the session is kept open; otherwise the session is terminated.
- This command applies to both the local console and Telnet connections.
- The timeout for Telnet cannot be disabled.
- Using the command without specifying a timeout restores the default setting.

EXAMPLE

To set the timeout to two minutes, enter this command:

```
Console(config-line)#exec-timeout 120
Console(config-line)#
```

login

This command enables password checking at login. Use the **no** form to disable password checking and allow connections without a password.

SYNTAX

login [**local**]

no login

local - Selects local password checking. Authentication is based on the user name specified with the username command.

DEFAULT SETTING

login local

COMMAND MODE

Line Configuration

COMMAND USAGE

- There are three authentication modes provided by the switch itself at login:
  - **login** selects authentication by a single global password as specified by the password line configuration command. When using this method, the management interface starts in Normal Exec (NE) mode.
  - **login local** selects authentication via the user name and password specified by the username command (i.e., default setting). When using this method, the management interface starts in Normal Exec (NE) or Privileged Exec (PE) mode, depending on the user's privilege level (0 or 15 respectively).
  - **no login** selects no authentication. When using this method, the management interface starts in Normal Exec (NE) mode.

- This command controls login authentication via the switch itself. To configure user names and passwords for remote authentication servers, you must use the RADIUS or TACACS software installed on those servers.

EXAMPLE

```
Console(config-line)#login local
Console(config-line)#
```

RELATED COMMANDS

username (555)
password (486)

parity

This command defines the generation of a parity bit. Use the **no** form to restore the default setting.

SYNTAX

parity {**none** | **even** | **odd**}

no parity

none - No parity

even - Even parity

odd - Odd parity

DEFAULT SETTING

No parity

COMMAND MODE

Line Configuration

COMMAND USAGE

Communication protocols provided by devices such as terminals and modems often require a specific parity bit setting.

EXAMPLE

To specify no parity, enter this command:

```
Console(config-line)#parity none
Console(config-line)#
```

password

This command specifies the password for a line. Use the **no** form to remove the password.

SYNTAX

password {**0** | **7**} *password*

no password

{**0** | **7**} - 0 means plain password, 7 means encrypted password

password - Character string that specifies the line password. (Maximum length: 32 characters plain text or encrypted, case sensitive)

DEFAULT SETTING

No password is specified.

COMMAND MODE

Line Configuration

COMMAND USAGE

- When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. You can use the password-thresh command to set the number of times a user can enter an incorrect password before the system terminates the line connection and returns the terminal to the idle state.

- The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

EXAMPLE

```
Console(config-line)#password 0 secret
Console(config-line)#
```

RELATED COMMANDS

login (484)
password-thresh (487)

password-thresh

This command sets the password intrusion threshold which limits the number of failed logon attempts. Use the **no** form to remove the threshold value.

SYNTAX

password-thresh [*threshold*]

no password-thresh

threshold - The number of allowed password attempts. (Range: 1-120; 0: no threshold)

DEFAULT SETTING

The default value is three attempts.

COMMAND MODE

Line Configuration

COMMAND USAGE

When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the silent-time command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface shuts down.

EXAMPLE

To set the password threshold to five attempts, enter this command:

```
Console(config-line)#password-thresh 5
Console(config-line)#
```

RELATED COMMANDS

silent-time (487)

silent-time

This command sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the password-thresh command. Use the **no** form to remove the silent time value.

SYNTAX

silent-time [*seconds*]

no silent-time

seconds - The number of seconds to disable console response. (Range: 0-65535; 0: 30 seconds)

DEFAULT SETTING

The default value is no silent-time.

COMMAND MODE
Line Configuration

EXAMPLE
To set the silent time to 60 seconds, enter this command:

```
Console(config-line)#silent-time 60
Console(config-line)#
```

RELATED COMMANDS
password-thresh (487)

speed
This command sets the terminal line's baud rate. This command sets both the transmit (to terminal) and receive (from terminal) speeds. Use the **no** form to restore the default setting.

SYNTAX
speed *bps*

no speed

bps - Baud rate in bits per second.
(Options: 9600, 19200, 38400 bps)

DEFAULT SETTING
115200 bps

COMMAND MODE
Line Configuration

COMMAND USAGE
Set the speed to match the baud rate of the device connected to the serial port. Some baud rates available on devices connected to the port might not be supported. The system indicates if the speed you selected is not supported.

EXAMPLE
To specify 38400 bps, enter this command:

```
Console(config-line)#speed 38400
Console(config-line)#
```

stopbits

This command sets the number of the stop bits transmitted per byte. Use the **no** form to restore the default setting.

SYNTAX

stopbits {**1** | **2**}

no stopbits

1 - One stop bit

2 - Two stop bits

DEFAULT SETTING

1 stop bit

COMMAND MODE

Line Configuration

EXAMPLE

To specify 2 stop bits, enter this command:

```
Console(config-line)#stopbits 2
Console(config-line)#
```

timeout login response

This command sets the interval that the system waits for a user to log into the CLI. Use the **no** form to restore the default setting.

SYNTAX

timeout login response [*seconds*]

no timeout login response

seconds - Integer that specifies the timeout interval. (Range: 0 - 300 seconds; 0: disabled)

DEFAULT SETTING

CLI: Disabled (0 seconds)
Telnet: 300 seconds

COMMAND MODE

Line Configuration

COMMAND USAGE

- If a login attempt is not detected within the timeout interval, the connection is terminated for the session.
- This command applies to both the local console and Telnet connections.
- The timeout for Telnet cannot be disabled.

- Using the command without specifying a timeout restores the default setting.

EXAMPLE

To set the timeout to two minutes, enter this command:

```
Console(config-line)#timeout login response 120
Console(config-line)#
```

disconnect

This command terminates an SSH, Telnet, or console connection.

SYNTAX

disconnect *session-id*

session-id – The session identifier for an SSH, Telnet or console connection. (Range: 0-4)

COMMAND MODE

Privileged Exec

COMMAND USAGE

Specifying session identifier "0" will disconnect the console connection. Specifying any other identifiers for an active session will disconnect an SSH or Telnet connection.

EXAMPLE

```
Console#disconnect 1
Console#
```

RELATED COMMANDS

show ssh (589)
show users (468)

show line

This command displays the terminal line's parameters.

SYNTAX

show line [**console** | **vty**]

console - Console terminal line.

vty - Virtual terminal for remote console access (i.e., Telnet).

DEFAULT SETTING

Shows all lines

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

To show all lines, enter this command:

```
Console#show line
 Console Configuration:
  Password Threshold : 3 times
  Inactive Timeout   : Disabled
  Login Timeout      : Disabled
  Silent Time        : Disabled
  Baud Rate          : Auto
  Data Bits          : 8
  Parity             : None
  Stop Bits          : 1

 VTY Configuration:
  Password Threshold : 3 times
  Inactive Timeout   : 600 sec.
  Login Timeout      : 300 sec.
Console#
```

EVENT LOGGING

This section describes commands used to configure event logging on the switch.

Table 44: Event Logging Commands

Command	Function	Mode
logging facility	Sets the facility type for remote logging of syslog messages	GC
logging history	Limits syslog messages saved to switch memory based on severity	GC
logging host	Adds a syslog server host IP address that will receive logging messages	GC
logging on	Controls logging of error messages	GC
logging trap	Limits syslog messages saved to a remote server based on severity	GC
clear log	Clears messages from the logging buffer	PE
show log	Displays log messages	PE
show logging	Displays the state of logging	PE

logging facility

This command sets the facility type for remote logging of syslog messages. Use the **no** form to return the type to the default.

SYNTAX

logging facility *type*

no logging facility

type - A number that indicates the facility used by the syslog server to dispatch log messages to an appropriate service. (Range: 16-23)

DEFAULT SETTING

23

COMMAND MODE

Global Configuration

COMMAND USAGE

The command specifies the facility type tag sent in syslog messages. (See RFC 3164.) This type has no effect on the kind of messages reported by the switch. However, it may be used by the syslog server to sort messages or to store messages in the corresponding database.

EXAMPLE

```
Console(config)#logging facility 19
Console(config)#
```

logging history

This command limits syslog messages saved to switch memory based on severity. The **no** form returns the logging of syslog messages to the default level.

SYNTAX

logging history {**flash** | **ram**} *level*

no logging history {**flash** | **ram**}

flash - Event history stored in flash memory (i.e., permanent memory).

ram - Event history stored in temporary RAM (i.e., memory flushed on power reset).

level - One of the levels listed below. Messages sent include the selected level down to level 0. (Range: 0-7)

Table 45: Logging Levels

Level	Severity Name	Description
7	debugging	Debugging messages
6	informational	Informational messages only
5	notifications	Normal but significant condition, such as cold start

Table 45: Logging Levels (Continued)

Level	Severity Name	Description
4	warnings	Warning conditions (e.g., return false, unexpected return)
3	errors	Error conditions (e.g., invalid input, default used)
2	critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
1	alerts	Immediate action needed
0	emergencies	System unusable

DEFAULT SETTING
Flash: errors (level 3 - 0)
RAM: debugging (level 7 - 0)

COMMAND MODE
Global Configuration

COMMAND USAGE
The message level specified for flash memory must be a higher priority (i.e., numerically lower) than that specified for RAM.

EXAMPLE

```
Console(config)#logging history ram 0
Console(config)#
```

logging host

This command adds a syslog server host IP address that will receive logging messages. Use the **no** form to remove a syslog server host.

SYNTAX

[**no**] **logging host** *host-ip-address*

host-ip-address - The IP address of a syslog server.

DEFAULT SETTING
None

COMMAND MODE
Global Configuration

COMMAND USAGE
- Use this command more than once to build up a list of host IP addresses.
- The maximum number of host IP addresses allowed is five.

EXAMPLE

```
Console(config)#logging host 10.1.0.3
Console(config)#
```

logging on

This command controls logging of error messages, sending debug or error messages to a logging process. The **no** form disables the logging process.

SYNTAX

[**no**] **logging on**

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

The logging process controls error messages saved to switch memory or sent to remote syslog servers. You can use the logging history command to control the type of error messages that are stored in memory. You can use the logging trap command to control the type of error messages that are sent to specified syslog servers.

EXAMPLE

```
Console(config)#logging on
Console(config)#
```

RELATED COMMANDS

logging history (492)
logging trap (494)
clear log (495)

logging trap

This command enables the logging of system messages to a remote server, or limits the syslog messages saved to a remote server based on severity. Use this command without a specified level to enable remote logging. Use the **no** form to disable remote logging.

SYNTAX

logging trap [**level** *level*]

no logging trap [**level**]

level - One of the syslog severity levels listed in the table on page 492. Messages sent include the selected level through level 0.

DEFAULT SETTING
Disabled
Level 7

COMMAND MODE
Global Configuration

COMMAND USAGE
- Using this command with a specified level enables remote logging and sets the minimum severity level to be saved.
- Using this command without a specified level also enables remote logging, but restores the minimum severity level to the default.

EXAMPLE
```
Console(config)#logging trap 4
Console(config)#
```

clear log
This command clears messages from the log buffer.

SYNTAX
clear log [**flash** | **ram**]

flash - Event history stored in flash memory (i.e., permanent memory).

ram - Event history stored in temporary RAM (i.e., memory flushed on power reset).

DEFAULT SETTING
Flash and RAM

COMMAND MODE
Privileged Exec

EXAMPLE
```
Console#clear log
Console#
```

RELATED COMMANDS
show log (496)

show log

This command displays the log messages stored in local memory.

SYNTAX

show log {**flash** | **ram**}

flash - Event history stored in flash memory (i.e., permanent memory).

ram - Event history stored in temporary RAM (i.e., memory flushed on power reset).

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

The following example shows the event message stored in RAM.

```
Console#show log ram
[1] 00:01:30 2001-01-01
   "VLAN 1 link-up notification."
   level: 6, module: 5, function: 1, and event no.: 1
[0] 00:01:30 2001-01-01
   "Unit 1, Port  1 link-up notification."
   level: 6, module: 5, function: 1, and event no.: 1
Console#
```

show logging

This command displays the configuration settings for logging messages to local switch memory, to an SMTP event handler, or to a remote syslog server.

SYNTAX

show logging {**flash** | **ram** | **sendmail** | **trap**}

flash - Displays settings for storing event messages in flash memory (i.e., permanent memory).

ram - Displays settings for storing event messages in temporary RAM (i.e., memory flushed on power reset).

sendmail - Displays settings for the SMTP event handler (page 501).

trap - Displays settings for the trap function.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

The following example shows that system logging is enabled, the message level for flash memory is "errors" (i.e., default level 3 - 0), and the message level for RAM is "debugging" (i.e., default level 7 - 0).

```
Console#show logging flash
Syslog logging:           Enabled
History logging in FLASH: level errors
Console#show logging ram
Syslog logging:           Enabled
History logging in RAM: level debugging
Console#
```

Table 46: show logging flash/ram - display description

Field	Description
Syslog logging	Shows if system logging has been enabled via the logging on command.
History logging in FLASH	The message level(s) reported based on the logging history command.
History logging in RAM	The message level(s) reported based on the logging history command.

The following example displays settings for the trap function.

```
Console#show logging trap
Syslog logging: Enable
REMOTELOG Status: disable
REMOTELOG Facility Type: Local use 7
REMOTELOG Level Type:        Debugging messages
REMOTELOG server IP Address: 1.2.3.4
REMOTELOG server IP Address: 0.0.0.0
REMOTELOG server IP Address: 0.0.0.0
REMOTELOG server IP Address: 0.0.0.0
REMOTELOG server IP Address: 0.0.0.0
Console#
```

Table 47: show logging trap - display description

Field	Description
Syslog logging	Shows if system logging has been enabled via the logging on command.
REMOTELOG status	Shows if remote logging has been enabled via the logging trap command.
REMOTELOG facility type	The facility type for remote logging of syslog messages as specified in the logging facility command.
REMOTELOG level type	The severity threshold for syslog messages sent to a remote server as specified in the logging trap command.
REMOTELOG server IP address	The address of syslog servers as specified in the logging host command.

RELATED COMMANDS

show logging sendmail (501)

SMTP ALERTS

These commands configure SMTP event handling, and forwarding of alert messages to the specified SMTP servers and email recipients.

Table 48: Event Logging Commands

Command	Function	Mode
logging sendmail	Enables SMTP event handling	GC
logging sendmail destination-email	Email recipients of alert messages	GC
logging sendmail host	SMTP servers to receive alert messages	GC
logging sendmail level	Severity threshold used to trigger alert messages	GC
logging sendmail source-email	Email address used for "From" field of alert messages	GC
show logging sendmail	Displays SMTP event handler settings	NE, PE

logging sendmail

This command enables SMTP event handling. Use the **no** form to disable this function.

SYNTAX

[**no**] **logging sendmail**

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#logging sendmail
Console(config)#
```

logging sendmail destination-email

This command specifies the email recipients of alert messages. Use the **no** form to remove a recipient.

SYNTAX

[**no**] **logging sendmail destination-email** *email-address*

email-address - The source email address used in alert messages. (Range: 1-41 characters)

DEFAULT SETTING
None

COMMAND MODE
Global Configuration

COMMAND USAGE
You can specify up to five recipients for alert messages. However, you must enter a separate command to specify each recipient.

EXAMPLE

```
Console(config)#logging sendmail destination-email ted@this-company.com
Console(config)#
```

logging sendmail host

This command specifies SMTP servers that will be sent alert messages. Use the **no** form to remove an SMTP server.

SYNTAX

[**no**] **logging sendmail host** *ip-address*

ip-address - IP address of an SMTP server that will be sent alert messages for event handling.

DEFAULT SETTING
None

COMMAND MODE
Global Configuration

COMMAND USAGE
- You can specify up to three SMTP servers for event handing. However, you must enter a separate command to specify each server.
- To send email alerts, the switch first opens a connection, sends all the email alerts waiting in the queue one by one, and finally closes the connection.
- To open a connection, the switch first selects the server that successfully sent mail during the last connection, or the first server configured by this command. If it fails to send mail, the switch selects the next server in the list and tries to send mail again. If it still fails, the system will repeat the process at a periodic interval. (A trap will be triggered if the switch cannot successfully open a connection.)

EXAMPLE

```
Console(config)#logging sendmail host 192.168.1.19
Console(config)#
```

logging sendmail level

This command sets the severity threshold used to trigger alert messages. Use the **no** form to restore the default setting.

SYNTAX

logging sendmail level level

no logging sendmail level

level - One of the system message levels (page 492). Messages sent include the selected level down to level 0. (Range: 0-7; Default: 7)

DEFAULT SETTING

Level 7

COMMAND MODE

Global Configuration

COMMAND USAGE

The specified level indicates an event threshold. All events at this level or higher will be sent to the configured email recipients. (For example, using Level 7 will report all events from level 7 to level 0.)

EXAMPLE

This example will send email alerts for system errors from level 3 through 0.

```
Console(config)#logging sendmail level 3
Console(config)#
```

logging sendmail source-email

This command sets the email address used for the "From" field in alert messages. Use the **no** form to restore the default value.

SYNTAX

logging sendmail source-email email-address

no logging sendmail source-email

email-address - The source email address used in alert messages. (Range: 1-41 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

You may use an symbolic email address that identifies the switch, or the address of an administrator responsible for the switch.

EXAMPLE

```
Console(config)#logging sendmail source-email bill@this-company.com
Console(config)#
```

show logging sendmail

This command displays the settings for the SMTP event handler.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
Console#show logging sendmail
SMTP servers
------------------------------------------------
192.168.1.19

SMTP Minimum Severity Level: 7

SMTP destination email addresses
------------------------------------------------
ted@this-company.com

SMTP Source Email Address: bill@this-company.com

SMTP Status: Enabled
Console#
```

TIME

The system clock can be dynamically set by polling a set of specified time servers (NTP or SNTP). Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. If the clock is not set, the switch will only record the time from the factory default set at the last bootup.

Table 49: Time Commands

Command	Function	Mode
SNTP Commands		
sntp client	Accepts time from specified time servers	GC
sntp poll	Sets the interval at which the client polls for time	GC
sntp server	Specifies one or more time servers	GC
show sntp	Shows current SNTP configuration settings	NE, PE
NTP Commands		
ntp authenticate	Enables authentication for NTP traffic	GC
ntp authentication-key	Configures authentication keys	GC
ntp client	Enables the NTP client for time updates from specified servers	GC

Table 49: Time Commands (Continued)

Command	Function	Mode
ntp server	Specifies NTP servers to poll for time updates	GC
show ntp	Shows current NTP configuration settings	NE, PE
Manual Configuration Commands		
clock summer-time (date)	Configures summer time* for the switch's internal clock	GC
clock summer-time (predefined)	Configures summer time* for the switch's internal clock	GC
clock summer-time (recurring)	Configures summer time* for the switch's internal clock	GC
clock timezone	Sets the time zone for the switch's internal clock	GC
clock timezone-predefined	Sets the time zone for the switch's internal clock using predefined time zone configurations	GC
calendar set	Sets the system date and time	PE
show calendar	Displays the current date and time setting	NE, PE

* Daylight savings time.

sntp client

This command enables SNTP client requests for time synchronization from NTP or SNTP time servers specified with the sntp server command. Use the **no** form to disable SNTP client requests.

SYNTAX

[**no**] **sntp client**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- The time acquired from time servers is used to record accurate dates and times for log events. Without SNTP, the switch only records the time starting from the factory default set at the last bootup (i.e., 00:00:00, Jan. 1, 2001).
- This command enables client time requests to time servers specified via the sntp server command. It issues time synchronization requests based on the interval set via the sntp poll command.

EXAMPLE

```
Console(config)#sntp server 10.1.0.19
Console(config)#sntp poll 60
Console(config)#sntp client
Console(config)#end
Console#show sntp
```

```
Current Time:  Dec 23 02:52:44 2002
Poll Interval: 60
Current Mode: unicast
SNTP Status : Enabled
SNTP Server 137.92.140.80 0.0.0.0 0.0.0.0
Current Server: 137.92.140.80
Console#
```

RELATED COMMANDS

sntp server (503)
sntp poll (503)
show sntp (504)

sntp poll

This command sets the interval between sending time requests when the switch is set to SNTP client mode. Use the **no** form to restore to the default.

SYNTAX

sntp poll *seconds*

no sntp poll

seconds - Interval between time requests. (Range: 16-16384 seconds)

DEFAULT SETTING

16 seconds

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#sntp poll 60
Console#
```

RELATED COMMANDS

sntp client (502)

sntp server

This command sets the IP address of the servers to which SNTP time requests are issued. Use the this command with no arguments to clear all time servers from the current list. Use the **no** form to clear all time servers from the current list, or to clear a specific server.

SYNTAX

sntp server [*ip1* [*ip2* [*ip3*]]]

no sntp server [*ip1* [*ip2* [*ip3*]]]

ip - IP address of an time server (NTP or SNTP). (Range: 1 - 3 addresses)

DEFAULT SETTING
None

COMMAND MODE
Global Configuration

COMMAND USAGE
This command specifies time servers from which the switch will poll for time updates when set to SNTP client mode. The client will poll the time servers in the order specified until a response is received. It issues time synchronization requests based on the interval set via the sntp poll command.

EXAMPLE

```
Console(config)#sntp server 10.1.0.19
Console#
```

RELATED COMMANDS
sntp client (502)
sntp poll (503)
show sntp (504)

show sntp
This command displays the current time and configuration settings for the SNTP client, and indicates whether or not the local time has been properly updated.

COMMAND MODE
Normal Exec, Privileged Exec

COMMAND USAGE
This command displays the current time, the poll interval used for sending time synchronization requests, and the current SNTP mode (i.e., unicast).

EXAMPLE

```
Console#show sntp
Current Time   : Nov  5 18:51:22 2006
Poll Interval  : 16 seconds
Current Mode   : Unicast
SNTP Status    : Enabled
SNTP Server    : 137.92.140.80 0.0.0.0 0.0.0.0
Current Server : 137.92.140.80
Console#
```

ntp authenticate

This command enables authentication for NTP client-server communications. Use the **no** form to disable authentication.

SYNTAX

[**no**] **ntp authenticate**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

You can enable NTP authentication to ensure that reliable updates are received from only authorized NTP servers. The authentication keys and their associated key number must be centrally managed and manually distributed to NTP servers and clients. The key numbers and key values must match on both the server and client.

EXAMPLE

```
Console(config)#ntp authenticate
Console(config)#
```

RELATED COMMANDS

ntp authentication-key (505)

ntp authentication-key

This command configures authentication keys and key numbers to use when NTP authentication is enabled. Use the **no** form of the command to clear a specific authentication key or all keys from the current list.

SYNTAX

ntp authentication-key *number* **md5** *key*

no ntp authentication-key [*number*]

number - The NTP authentication key ID number. (Range: 1-65535)

md5 - Specifies that authentication is provided by using the message digest algorithm 5.

key - An MD5 authentication key string. The key string can be up to 32 case-sensitive printable ASCII characters (no spaces).

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- The key number specifies a key value in the NTP authentication key list. Up to 255 keys can be configured on the switch. Re-enter this command for each server you want to configure.
- Note that NTP authentication key numbers and values must match on both the server and client.
- NTP authentication is optional. When enabled with the **ntp authenticate** command, you must also configure at least one key number using this command.
- Use the **no** form of this command without an argument to clear all authentication keys in the list.

EXAMPLE

```
Console(config)#ntp authentication-key 45 md5 thisiskey45
Console(config)#
```

RELATED COMMANDS

ntp authenticate (505)

ntp client

This command enables NTP client requests for time synchronization from NTP time servers specified with the **ntp servers** command. Use the **no** form to disable NTP client requests.

SYNTAX

[**no**] **ntp client**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- The SNTP and NTP clients cannot be enabled at the same time. First disable the SNTP client before using this command.
- The time acquired from time servers is used to record accurate dates and times for log events. Without NTP, the switch only records the time starting from the factory default set at the last bootup (i.e., 00:00:00, Jan. 1, 2001).
- This command enables client time requests to time servers specified via the **ntp servers** command. It issues time synchronization requests based on the interval set via the **ntp poll** command.

EXAMPLE

```
Console(config)#ntp client
Console(config)#
```

RELATED COMMANDS

sntp client (502)
ntp server (507)

ntp server

This command sets the IP addresses of the servers to which NTP time requests are issued. Use the **no** form of the command to clear a specific time server or all servers from the current list.

SYNTAX

ntp server *ip-address* [**version** *number*] [**key** *key-number*]

no ntp server [*ip-address*]

ip-address - IP address of an NTP time server.

number - The NTP version number supported by the server. (Range: 1-3)

key-number - The number of an authentication key to use in communications with the server. (Range: 1-65535)

DEFAULT SETTING

Version number: 3

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command specifies time servers that the switch will poll for time updates when set to NTP client mode. It issues time synchronization requests based on the interval set with the **ntp poll** command. The client will poll all the time servers configured, the responses received are filtered and compared to determine the most reliable and accurate time update for the switch.
- You can configure up to 50 NTP servers on the switch. Re-enter this command for each server you want to configure.
- NTP authentication is optional. If enabled with the **ntp authenticate** command, you must also configure at least one key number using the **ntp authentication-key** command.
- Use the **no** form of this command without an argument to clear all configured servers in the list.

EXAMPLE

```
Console(config)#ntp server 192.168.3.20
Console(config)#ntp server 192.168.3.21
Console(config)#ntp server 192.168.4.22 version 2
Console(config)#ntp server 192.168.5.23 version 3 key 19
Console(config)#
```

RELATED COMMANDS

ntp client (506)
show ntp (508)

show ntp

This command displays the current time and configuration settings for the NTP client, and indicates whether or not the local time has been properly updated.

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

This command displays the current time, the poll interval used for sending time synchronization requests, and the current NTP mode (i.e., unicast).

EXAMPLE

```
Console#show ntp
Current Time             : Jan  1 00:09:30 2001
Polling                  : 1024 seconds
Current Mode             : unicast
NTP Status               : Enabled
NTP Authenticate Status  : Enabled
Last Update NTP Server   : 0.0.0.0        Port: 0
Last Update Time         : Dec 31 00:00:00 2000 UTC
NTP Server 192.168.3.20 version 3
NTP Server 192.168.3.21 version 3
NTP Server 192.168.3.22 version 2
NTP Server 192.168.4.50 version 3 key 30
NTP Server 192.168.5.35 version 3 key 19
NTP Authentication-Key 12 md5 156S46Q24142414222711K66N80 7
NTP Authentication-Key 19 md5 Q33O16Q6338241J022S29Q731K7 7
NTP Authentication-Key 30 md5 D2V8777I51K1132K3552L26R6141O4 7
NTP Authentication-Key 45 md5 3U865531O13K38F0R8 7
NTP Authentication-Key 125 md5 A48S2810327947M76 7
Console#
```

clock summer-time (date)

This command sets the start, end, and offset times of summer time (daylight savings time) for the switch on a one-time basis. Use the **no** form to disable summer time.

SYNTAX

clock summer-time *name* **date** *b-month b-day b-year b-hour b-minute e-month e-day e-year e-hour e-minute offset*

no clock summer-time

name - Name of the time zone while summer time is in effect, usually an acronym. (Range: 1-30 characters)

b-month - The month when summer time will begin. (Options: **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**)

b-day - The day summer time will begin. (Options: **sunday** | **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday**)

b-year- The year summer time will begin.

b-hour - The hour summer time will begin. (Range: 0-23 hours)

b-minute - The minute summer time will begin. (Range: 0-59 minutes)

e-month - The month when summer time will end. (Options: **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**)

e-day - The day summer time will end. (Options: **sunday** | **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday**)

e-year - The year summer time will end.

e-hour - The hour summer time will end. (Range: 0-23 hours)

e-minute - The minute summer time will end. (Range: 0-59 minutes)

offset - Summer time offset from the regular time zone, in minutes. (Range: 0-99 minutes)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Summer Time, or Daylight Savings Time (DST). Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn.

- This command sets the summer-time time zone relative to the currently configured time zone. To specify a time corresponding to your local time when summer time is in effect, you must indicate the number of minutes your summer-time time zone deviates from your regular time zone.

EXAMPLE

```
Console(config)#clock summer-time DEST date april 1 2007 23 23 april 23 2007
  23 23 60
Console(config)#
```

RELATED COMMANDS

show sntp (504)

clock summer-time (predefined)

This command configures the summer time (daylight savings time) status and settings for the switch using predefined configurations for several major regions of the world. Use the **no** form to disable summer time.

SYNTAX

clock summer-time *name* **predefined** [**australia** | **europe** | **new-zealand** | **usa**]

no clock summer-time

name - Name of the timezone while summer time is in effect, usually an acronym. (Range: 1-30 characters)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Summer Time, or Daylight Savings Time (DST). Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn.

- This command sets the summer-time time relative to the configured time zone. To specify the time corresponding to your local time when summer time is in effect, select the predefined summer-time time zone appropriate for your location, or manually configure summer time if these predefined configurations do not apply to your location (see clock summer-time (date) or clock summer-time (recurring).

Table 50: Predefined Summer-Time Parameters

Region	Start Time, Day, Week, & Month	End Time, Day, Week, & Month	Rel. Offset
Australia	00:00:00, Sunday, Week 5 of October	23:59:59, Sunday, Week 5 of March	60 min
Europe	00:00:00, Sunday, Week 5 of March	23:59:59, Sunday, Week 5 of October	60 min
New Zealand	00:00:00, Sunday, Week 1 of October	23:59:59, Sunday, Week 3 of March	60 min
Australia	00:00:00, Sunday, Week 5 of October	23:59:59, Sunday, Week 5 of March	60 min

EXAMPLE

```
Console(config)#clock summer-time MESZ predefined europe
Console(config)#
```

RELATED COMMANDS

show sntp (504)

clock summer-time (recurring)

This command allows the user to manually configure the start, end, and offset times of summer time (daylight savings time) for the switch on a recurring basis. Use the **no** form to disable summer-time.

SYNTAX

clock summer-time *name* **recurring** *b-week b-day b-month b-hour b-minute e-week e-day e-month e-hour e-minute offset*

no clock summer-time

name - Name of the timezone while summer time is in effect, usually an acronym. (Range: 1-30 characters)

b-week - The week of the month when summer time will begin. (Range: 1-5)

b-day - The day of the week when summer time will begin. (Options: **sunday** | **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday**)

b-month - The month when summer time will begin. (Options: **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**)

b-hour - The hour when summer time will begin. (Range: 0-23 hours)

b-minute - The minute when summer time will begin. (Range: 0-59 minutes)

e-week - The week of the month when summer time will end. (Range: 1-5)

e-day - The day of the week summer time will end. (Options: **sunday** | **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday**)

e-month - The month when summer time will end. (Options: **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**)

e-hour - The hour when summer time will end. (Range: 0-23 hours)

e-minute - The minute when summer time will end. (Range: 0-59 minutes)

offset - Summer-time offset from the regular time zone, in minutes. (Range: 0-99 minutes)

DEFAULT SETTING
Disabled

COMMAND MODE
Global Configuration

COMMAND USAGE
- In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Summer Time, or Daylight Savings Time (DST). Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn.

- This command sets the summer-time time zone relative to the currently configured time zone. To display a time corresponding to your local time when summer time is in effect, you must indicate the number of minutes your summer-time time zone deviates from your regular time zone.

EXAMPLE
```
Console(config)#clock summer-time MESZ recurring 1 friday june 23 59 3
  saturday september 2 55 60
Console(config)#
```

RELATED COMMANDS
show sntp (504)

clock timezone

This command sets the time zone for the switch's internal clock.

SYNTAX

clock timezone *name* **hour** *hours* **minute** *minutes* {**before-utc** | **after-utc**}

name - Name of timezone, usually an acronym. (Range: 1-30 characters)

hours - Number of hours before/after UTC. (Range: 0-12 hours before UTC, 0-13 hours after UTC)

minutes - Number of minutes before/after UTC. (Range: 0-59 minutes)

before-utc - Sets the local time zone before (east) of UTC.

after-utc - Sets the local time zone after (west) of UTC.

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

This command sets the local time zone relative to the Coordinated Universal Time (UTC, formerly Greenwich Mean Time or GMT), based on the earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

EXAMPLE

```
Console(config)#clock timezone Japan hours 8 minute 0 after-UTC
Console(config)#
```

RELATED COMMANDS

show sntp (504)

clock timezone-predefined

This command uses predefined time zone configurations to set the time zone for the switch's internal clock. Use the **no** form to restore the default.

SYNTAX

clock timezone-predefined *offset-city*

no clock timezone-predefined

offset - Select the offset from GMT. (Range: GMT-0100 - GMT-1200; GMT-Greenwich-Mean-Time; GMT+0100 - GMT+1300)

city - Select the city associated with the chosen GMT offset. After the offset has been entered, use the tab-complete function to display the available city options.

DEFAULT SETTING
GMT-Greenwich-Mean-Time-Dublin,Edinburgh,Lisbon,London

COMMAND MODE
Global Configuration

COMMAND USAGE
This command sets the local time zone relative to the Coordinated Universal Time (UTC, formerly Greenwich Mean Time or GMT), based on the earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

EXAMPLE

```
Console(config)#clock timezone-predefined GMT-0930-Taiohae
Console(config)#
```

RELATED COMMANDS
show sntp (504)

calendar set

This command sets the system clock. It may be used if there is no time server on your network, or if you have not configured the switch to receive signals from a time server.

SYNTAX

calendar set *hour min sec* {*day month year* | *month day year*}

hour - Hour in 24-hour format. (Range: 0 - 23)

min - Minute. (Range: 0 - 59)

sec - Second. (Range: 0 - 59)

day - Day of month. (Range: 1 - 31)

month - **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**

year - Year (4-digit). (Range: 2001 - 2100)

DEFAULT SETTING
None

COMMAND MODE
Privileged Exec

COMMAND USAGE
Note that when SNTP is enabled, the system clock cannot be manually configured.

EXAMPLE

This example shows how to set the system clock to 15:12:34, February 1st, 2002.

```
Console#calendar set 15:12:34 1 February 2002
Console#
```

show calendar

This command displays the system clock.

DEFAULT SETTING

None

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
Console#show calendar
 15:12:34 February 1 2002
Console#
```

TIME RANGE

This section describes the commands used to sets a time range for use by other functions, such as Access Control Lists.

Table 51: Time Range Commands

Command	Function	Mode
time-range	Specifies the name of a time range, and enters time range configuration mode	GC
absolute	Sets the time range for the execution of a command	TR
periodic	Sets the time range for the periodic execution of a command	TR
show time-range	Shows configured time ranges.	PE

time-range

This command specifies the name of a time range, and enters time range configuration mode. Use the **no** form to remove a previously specified time range.

SYNTAX

[**no**] **time-range** *name*

name - Name of the time range. (Range: 1-30 characters)

DEFAULT SETTING
None

COMMAND MODE
Global Configuration

COMMAND USAGE
This command sets a time range for use by other functions, such as Access Control Lists.

EXAMPLE

```
Console(config)#time-range r&d
Console(config-time-range)#
```

RELATED COMMANDS
Access Control Lists (659)

absolute

This command sets the time range for the execution of a command. Use the **no** form to remove a previously specified time.

SYNTAX

absolute start *hour minute day month year*
[**end** *hour minutes day month year*]

absolute end *hour minutes day month year*

no absolute

hour - Hour in 24-hour format. (Range: 0-23)

minute - Minute. (Range: 0-59)

day - Day of month. (Range: 1-31)

month - **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**

year - Year (4-digit). (Range: 2009-2109)

DEFAULT SETTING
None

COMMAND MODE
Time Range Configuration

COMMAND USAGE
If a time range is already configured, you must use the **no** form of this command to remove the current entry prior to configuring a new time range.

EXAMPLE

This example configures the time for the single occurrence of an event.

```
Console(config)#time-range r&d
Console(config-time-range)#absolute start 1 1 1 april 2009 end 2 1 1 april
  2009
Console(config-time-range)#
```

periodic

This command sets the time range for the periodic execution of a command. Use the **no** form to remove a previously specified time range.

SYNTAX

[**no**] **periodic** {**daily** | **friday** | **monday** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday** | **weekdays** | **weekend**} *hour minute* to {**daily** | **friday** | **monday** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday** | **weekdays** | **weekend** | *hour minute*}

daily - Daily

friday - Friday

monday - Monday

saturday - Saturday

sunday - Sunday

thursday - Thursday

tuesday - Tuesday

wednesday - Wednesday

weekdays - Weekdays

weekend - Weekends

hour - Hour in 24-hour format. (Range: 0-23)

minute - Minute. (Range: 0-59)

DEFAULT SETTING

None

COMMAND MODE

Time Range Configuration

EXAMPLE

This example configures a time range for the periodic occurrence of an event.

```
Console(config)#time-range sales
Console(config-time-range)#periodic daily 1 1 to 2 1
Console(config-time-range)#
```

show time-range

This command shows configured time ranges.

SYNTAX

show time-range [*name*]

name - Name of the time range. (Range: 1-30 characters)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#showtime-range r&d
 Time-range r&d:
   absolute start 01:01 01 April 2009
   periodic    Daily 01:01 to    Daily 02:01
   periodic    Daily 02:01 to    Daily 03:01
Console#
```

SWITCH CLUSTERING

Switch Clustering is a method of grouping switches together to enable centralized management through a single unit. Switches that support clustering can be grouped together regardless of physical location or switch type, as long as they are connected to the same local network.

Table 52: Switch Cluster Commands

Command	Function	Mode
cluster	Configures clustering on the switch	GC
cluster commander	Configures the switch as a cluster Commander	GC
cluster ip-pool	Sets the cluster IP address pool for Members	GC
cluster member	Sets Candidate switches as cluster members	GC
rcommand	Provides configuration access to Member switches	PE
show cluster	Displays the switch clustering status	PE
show cluster members	Displays current cluster Members	PE
show cluster candidates	Displays current cluster Candidates in the network	PE

Using Switch Clustering

- A switch cluster has a primary unit called the "Commander" which is used to manage all other "Member" switches in the cluster. The management station can use either Telnet or the web interface to communicate directly with the Commander through its IP address, and

then use the Commander to manage the Member switches through the cluster's "internal" IP addresses.

- Clustered switches must be in the same Ethernet broadcast domain. In other words, clustering only functions for switches which can pass information between the Commander and potential Candidates or active Members through VLAN 4093.

- Once a switch has been configured to be a cluster Commander, it automatically discovers other cluster-enabled switches in the network. These "Candidate" switches only become cluster Members when manually selected by the administrator through the management station.

NOTE: Cluster Member switches can be managed either through a Telnet connection to the Commander, or through a web management connection to the Commander. When using a console connection, from the Commander CLI prompt, use the rcommand to connect to the Member switch.

cluster

This command enables clustering on the switch. Use the **no** form to disable clustering.

SYNTAX

[**no**] **cluster**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- To create a switch cluster, first be sure that clustering is enabled on the switch (the default is enabled), then set the switch as a Cluster Commander. Set a Cluster IP Pool that does not conflict with any other IP subnets in the network. Cluster IP addresses are assigned to switches when they become Members and are used for communication between Member switches and the Commander.

- Switch clusters are limited to the same Ethernet broadcast domain.

- There can be up to 100 candidates and 36 member switches in one cluster.

- A switch can only be a Member of one cluster.

- Configured switch clusters are maintained across power resets and network changes.

EXAMPLE

```
Console(config)#cluster
Console(config)#
```

cluster commander

This command enables the switch as a cluster Commander. Use the **no** form to disable the switch as cluster Commander.

SYNTAX

[**no**] **cluster commander**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- Once a switch has been configured to be a cluster Commander, it automatically discovers other cluster-enabled switches in the network. These "Candidate" switches only become cluster Members when manually selected by the administrator through the management station.
- Cluster Member switches can be managed through a Telnet connection to the Commander. From the Commander CLI prompt, use the rcommand id command to connect to the Member switch.

EXAMPLE

```
Console(config)#cluster commander
Console(config)#
```

cluster ip-pool

This command sets the cluster IP address pool. Use the **no** form to reset to the default address.

SYNTAX

cluster ip-pool *ip-address*

no cluster ip-pool

ip-address - The base IP address for IP addresses assigned to cluster Members. The IP address must start 10.x.x.x.

DEFAULT SETTING

10.254.254.1

COMMAND MODE

Global Configuration

COMMAND USAGE

- An "internal" IP address pool is used to assign IP addresses to Member switches in the cluster. Internal cluster IP addresses are in the form 10.*x.x.member-ID*. Only the base IP address of the pool needs to be set since Member IDs can only be between 1 and 36.
- Set a Cluster IP Pool that does not conflict with addresses in the network IP subnet. Cluster IP addresses are assigned to switches when they become Members and are used for communication between Member switches and the Commander.
- You cannot change the cluster IP pool when the switch is currently in Commander mode. Commander mode must first be disabled.

EXAMPLE

```
Console(config)#cluster ip-pool 10.2.3.4
Console(config)#
```

cluster member

This command configures a Candidate switch as a cluster Member. Use the **no** form to remove a Member switch from the cluster.

SYNTAX

cluster member mac-address *mac-address* **id** *member-id*

no cluster member id *member-id*

mac-address - The MAC address of the Candidate switch.

member-id - The ID number to assign to the Member switch. (Range: 1-36)

DEFAULT SETTING

No Members

COMMAND MODE

Global Configuration

COMMAND USAGE

- The maximum number of cluster Members is 36.
- The maximum number of cluster Candidates is 100.

EXAMPLE

```
Console(config)#cluster member mac-address 00-12-34-56-78-9a id 5
Console(config)#
```

rcommand

This command provides access to a cluster Member CLI for configuration.

SYNTAX

rcommand id *member-id*

member-id - The ID number of the Member switch. (Range: 1-36)

COMMAND MODE

Privileged Exec

COMMAND USAGE

- This command only operates through a Telnet connection to the Commander switch. Managing cluster Members using the local console CLI on the Commander is not supported.
- There is no need to enter the username and password for access to the Member switch CLI.

EXAMPLE

```
Console#rcommand id 1

      CLI session with the ES-3024GP is opened.
      To end the CLI session, enter [Exit].

Vty-0#
```

show cluster

This command shows the switch clustering configuration.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show cluster
Role                 : commander
Interval Heartbeat   : 30
Heartbeat Loss Count : 3 seconds
Number of Members    : 1
Number of Candidates : 2
Console#
```

show cluster members

This command shows the current switch cluster members.

COMMAND MODE
Privileged Exec

EXAMPLE

```
Console#show cluster members
Cluster Members:
ID          : 1
Role        : Active member
IP Address  : 10.254.254.2
MAC Address : 00-E0-0C-00-00-FE
Description : Edge-Core FE L2 Switch ES3528M

Console#
```

show cluster candidates

This command shows the discovered Candidate switches in the network.

COMMAND MODE
Privileged Exec

EXAMPLE

```
Console#show cluster candidates
Cluster Candidates:
Role            MAC Address       Description
--------------- ----------------- ---------------------------------------
Active member   00-E0-0C-00-00-FE ES-3024GP Managed GE POE Switch
CANDIDATE       00-12-CF-0B-47-A0 ES-3024GP Managed GE POE Switch
Console#
```

UPnP

Universal Plug and Play (UPnP) is a set of protocols that allows devices to connect seamlessly and simplifies the deployment of home and office networks. UPnP achieves this by issuing UPnP device control protocols designed upon open, Internet-based communication standards.

The commands described in this section allow the switch to advertise itself as a UPnP compliant device. When discovered by a host device, basic information about this switch can be displayed, and the web management interface accessed.

Table 53: UPnP Commands

Command	Function	Mode
upnp device	Enables/disables UPnP on the network	GC
upnp device ttl	Sets the time-to-live (TTL) value.	GC

Table 53: UPnP Commands (Continued)

Command	Function	Mode
upnp device advertise duration	Sets the advertisement duration of the device	GC
show upnp	Displays UPnP status and parameters	PE

upnp device

This command enables UPnP on the device. Use the **no** form to disable UPnP.

SYNTAX

[**no**] **upnp device**

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

COMMAND USAGE

You must enable UPnP before you can configure time-out settings for sending UPnP messages.

EXAMPLE

In the following example, UPnP is enabled on the device.

```
Console(config)#upnp device
Console(config)#
```

RELATED COMMANDS

upnp device ttl (524)
upnp device advertise duration (525)

upnp device ttl

This command sets the time-to-live (TTL) value for sending of UPnP messages from the device.

SYNTAX

upnp device ttl *value*

value - The number of router hops a UPnP packet can travel before it is discarded. (Range:1-255)

DEFAULT SETTING

4

COMMAND MODE

Global Configuration

COMMAND USAGE

UPnP devices and control points must be within the local network, that is within the TTL value for multicast messages.

EXAMPLE

In the following example, the TTL is set to 6.

```
Console(config)#upnp device ttl 6
Console(config)#
```

upnp device advertise duration

This command sets the duration for which a device will advertise its presence on the local network.

SYNTAX

upnp device advertise duration *value*

value - A time out value expressed in seconds. (Range: 6-86400 seconds)

DEFAULT SETTING

100 seconds

COMMAND MODE

Global Configuration

EXAMPLE

In the following example, the device advertise duration is set to 200 seconds.

```
Console(config)#upnp device advertise duration 200
Console(config)#
```

RELATED COMMANDS

upnp device ttl (524)

show upnp

This command displays the UPnP management status and time out settings.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show upnp
UPnP global settings:
 Status:                Enabled
 Advertise duration:    200
```

```
 TTL:                    20
Console#
```

22 SNMP COMMANDS

Controls access to this switch from management stations using the Simple Network Management Protocol (SNMP), as well as the error types sent to trap managers.

SNMP Version 3 also provides security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree. To use SNMPv3, first set an SNMP engine ID (or accept the default), specify read and write access views for the MIB tree, configure SNMP user groups with the required security model (i.e., SNMP v1, v2c or v3) and security level (i.e., authentication and privacy), and then assign SNMP users to these groups, along with their specific authentication and privacy passwords.

Table 54: SNMP Commands

Command	Function	Mode
General SNMP Commands		
snmp-server	Enables the SNMP agent	GC
snmp-server community	Sets up the community access string to permit access to SNMP commands	GC
snmp-server contact	Sets the system contact string	GC
snmp-server location	Sets the system location string	GC
show snmp	Displays the status of SNMP communications	NE, PE
SNMPv3 Commands		
snmp-server engine-id	Sets the SNMP engine ID	GC
snmp-server group	Adds an SNMP group, mapping users to views	GC
snmp-server user	Adds a user to an SNMP group	GC
snmp-server view	Adds an SNMP view	GC
show snmp engine-id	Shows the SNMP engine ID	PE
show snmp group	Shows the SNMP groups	PE
show snmp user	Shows the SNMP users	PE
show snmp view	Shows the SNMP views	PE
SNMP Trap Commands		
snmp-server enable traps	Enables the device to send SNMP traps (i.e., SNMP notifications)	GC
snmp-server host	Specifies the recipient of an SNMP notification operation	GC
MAC Notification Commands		
snmp-server enable traps mac-notification	Globally enables traps when changes occur for dynamic addresses in the MAC address table	GC

Table 54: SNMP Commands (Continued)

Command	Function	Mode
snmp-server enable port-traps mac-notification	Sends a trap when changes occur to dynamic addresses in the MAC address table for an interface	IC
show snmp-server enable port-traps interface	Shows the trap configuration for changes to dynamic entries in the MAC address table for an interface	PE
ATC Trap Commands		
snmp-server enable port-traps atc broadcast-alarm-clear	Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered	IC (Port)
snmp-server enable port-traps atc broadcast-alarm-fire	Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control	IC (Port)
snmp-server enable port-traps atc broadcast-control-apply	Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control and the apply timer expires	IC (Port)
snmp-server enable port-traps atc broadcast-control-release	Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires	IC (Port)
snmp-server enable port-traps atc multicast-alarm-clear	Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered	IC (Port)
snmp-server enable port-traps atc multicast-alarm-fire	Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control	IC (Port)
snmp-server enable port-traps atc multicast-control-apply	Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control and the apply timer expires	IC (Port)
snmp-server enable port-traps atc multicast-control-release	Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires	IC (Port)

snmp-server

This command enables the SNMPv3 engine and services for all management clients (i.e., versions 1, 2c, 3). Use the **no** form to disable the server.

SYNTAX

[**no**] **snmp-server**

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#snmp-server
Console(config)#
```

snmp-server community

This command defines community access strings used to authorize management access by clients using SNMP v1 or v2c. Use the **no** form to remove the specified community string.

SYNTAX

snmp-server community *string* [**ro** | **rw**]

no snmp-server community *string*

string - Community string that acts like a password and permits access to the SNMP protocol. (Maximum length: 32 characters, case sensitive; Maximum number of strings: 5)

ro - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.

rw - Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

DEFAULT SETTING

- public - Read-only access. Authorized management stations are only able to retrieve MIB objects.
- private - Read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#snmp-server community alpha rw
Console(config)#
```

snmp-server contact

This command sets the system contact string. Use the **no** form to remove the system contact information.

SYNTAX

snmp-server contact *string*

no snmp-server contact

string - String that describes the system contact information. (Maximum length: 255 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#snmp-server contact Paul
Console(config)#
```

RELATED COMMANDS

snmp-server location (530)

snmp-server location

This command sets the system location string. Use the **no** form to remove the location string.

SYNTAX

snmp-server location *text*

no snmp-server location

text - String that describes the system location. (Maximum length: 255 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#snmp-server location WC-19
Console(config)#
```

RELATED COMMANDS

snmp-server contact (529)

show snmp

This command can be used to check the status of SNMP communications.

DEFAULT SETTING

None

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

This command provides information on the community access strings, counter information for SNMP input and output protocol data units, and whether or not SNMP logging has been enabled with the **snmp-server enable traps** command.

EXAMPLE

```
Console#show snmp

SNMP Agent : Enabled

SNMP Traps :
            Authentication : Enabled
       User Authentication : Enabled
              Link-up-down : Enabled
          MAC-notification : Enabled
 MAC-notification interval : 10 second(s)

SNMP Communities :
   1. public, and the access level is read-only
   2. private, and the access level is read/write

0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
0 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs

SNMP Logging: Disabled
Console#
```

snmp-server engine-id

This command configures an identification string for the SNMPv3 engine. Use the **no** form to restore the default.

SYNTAX

snmp-server engine-id {**local** | **remote** {*ip-address*}} *engineid-string*

no snmp-server engine-id {**local** | **remote** {*ip-address*}}

local - Specifies the SNMP engine on this switch.

remote - Specifies an SNMP engine on a remote device.

ip-address - The Internet address of the remote device.

engineid-string - String identifying the engine ID. (Range: 1-26 hexadecimal characters)

DEFAULT SETTING

A unique engine ID is automatically generated by the switch based on its MAC address.

COMMAND MODE
Global Configuration

COMMAND USAGE
- An SNMP engine is an independent SNMP agent that resides either on this switch or on a remote device. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.

- A remote engine ID is required when using SNMPv3 informs. (See the snmp-server host command.) The remote engine ID is used to compute the security digest for authentication and encryption of packets passed between the switch and a user on the remote host. SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it.

- Trailing zeroes need not be entered to uniquely specify a engine ID. In other words, the value "0123456789" is equivalent to "0123456789" followed by 16 zeroes for a local engine ID.

- A local engine ID is automatically generated that is unique to the switch. This is referred to as the default engine ID. If the local engine ID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users (page 534).

EXAMPLE
```
Console(config)#snmp-server engine-id local 1234567890
Console(config)#snmp-server engineID remote 9876543210 192.168.1.19
Console(config)#
```

RELATED COMMANDS
snmp-server host (540)

snmp-server group

This command adds an SNMP group, mapping SNMP users to SNMP views. Use the **no** form to remove an SNMP group.

SYNTAX

snmp-server group *groupname*
{**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}}
[**read** *readview*] [**write** *writeview*] [**notify** *notifyview*]

no snmp-server group *groupname*

groupname - Name of an SNMP group. (Range: 1-32 characters)

v1 | **v2c** | **v3** - Use SNMP version 1, 2c or 3.

auth | **noauth** | **priv** - This group uses SNMPv3 with authentication, no authentication, or with authentication and privacy. See "Simple Network Management Protocol" for further information about these authentication and encryption options.

readview - Defines the view for read access. (1-32 characters)

writeview - Defines the view for write access. (1-32 characters)

notifyview - Defines the view for notifications. (1-32 characters)

DEFAULT SETTING

Default groups: public[14] (read only), private[15] (read/write)
readview - Every object belonging to the Internet OID space (1).
writeview - Nothing is defined.
notifyview - Nothing is defined.

COMMAND MODE

Global Configuration

COMMAND USAGE

- A group sets the access policy for the assigned users.
- When authentication is selected, the MD5 or SHA algorithm is used as specified in the snmp-server user command.
- When privacy is selected, the DES 56-bit algorithm is used for data encryption.
- For additional information on the notification messages supported by this switch, see Table 10, "Supported Notification Messages." Also, note that the authentication, link-up and link-down messages are legacy traps and must therefore be enabled in conjunction with the snmp-server enable traps command.

EXAMPLE

```
Console(config)#snmp-server group r&d v3 auth write daily
Console(config)#
```

14. No view is defined.
15. Maps to the defaultview.

snmp-server user

This command adds a user to an SNMP group, restricting the user to a specific SNMP Read, Write, or Notify View. Use the **no** form to remove a user from an SNMP group.

SYNTAX

snmp-server user *username groupname* [**remote** *ip-address*] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password* [**priv des56** *priv-password*]]

no snmp-server user *username* {**v1** | **v2c** | **v3** | **remote**}

username - Name of user connecting to the SNMP agent. (Range: 1-32 characters)

groupname - Name of an SNMP group to which the user is assigned. (Range: 1-32 characters)

remote - Specifies an SNMP engine on a remote device.

ip-address - The Internet address of the remote device.

v1 | **v2c** | **v3** - Use SNMP version 1, 2c or 3.

encrypted - Accepts the password as encrypted input.

auth - Uses SNMPv3 with authentication.

md5 | **sha** - Uses MD5 or SHA authentication.

auth-password - Authentication password. Enter as plain text if the **encrypted** option is not used. Otherwise, enter an encrypted password. (A minimum of eight characters is required.)

priv des56 - Uses SNMPv3 with privacy with DES56 encryption.

priv-password - Privacy password. Enter as plain text if the **encrypted** option is not used. Otherwise, enter an encrypted password.

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- Local users (i.e., the command does not specify a remote engine identifier) must be configured to authorize management access for SNMPv3 clients, or to identify the source of SNMPv3 trap messages sent from the local switch.
- Remote users (i.e., the command specifies a remote engine identifier) must be configured to identify the source of SNMPv3 inform messages sent from the local switch.
- The SNMP engine ID is used to compute the authentication/privacy digests from the password. You should therefore configure the engine ID with the snmp-server engine-id command before using this configuration command.

- Before you configure a remote user, use the snmp-server engine-id command to specify the engine ID for the remote device where the user resides. Then use the **snmp-server user** command to specify the user and the IP address for the remote device where the user resides. The remote agent's SNMP engine ID is used to compute authentication/privacy digests from the user's password. If the remote engine ID is not first configured, the **snmp-server user** command specifying a remote user will fail.

- SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it.

EXAMPLE

```
Console(config)#snmp-server user steve group r&d v3 auth md5 greenpeace priv
  des56 einstien
Console(config)#snmp-server user mark group r&d remote 192.168.1.19 v3 auth
  md5 greenpeace priv des56 einstien
Console(config)#
```

snmp-server view

This command adds an SNMP view which controls user access to the MIB. Use the **no** form to remove an SNMP view.

SYNTAX

snmp-server view *view-name oid-tree* {**included** | **excluded**}

no snmp-server view *view-name*

view-name - Name of an SNMP view. (Range: 1-32 characters)

oid-tree - Object identifier of a branch within the MIB tree. Wild cards can be used to mask a specific portion of the OID string. (Refer to the examples.)

included - Defines an included view.

excluded - Defines an excluded view.

DEFAULT SETTING

defaultview (includes access to the entire MIB tree)

COMMAND MODE

Global Configuration

COMMAND USAGE

- Views are used in the snmp-server group command to restrict user access to specified portions of the MIB tree.

- The predefined view "defaultview" includes access to the entire MIB tree.

EXAMPLES

This view includes MIB-2.

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included
Console(config)#
```

This view includes the MIB-2 interfaces table, ifDescr. The wild card is used to select all the index values in this table.

```
Console(config)#snmp-server view ifEntry.2 1.3.6.1.2.1.2.2.1.*.2 included
Console(config)#
```

This view includes the MIB-2 interfaces table, and the mask selects all index entries.

```
Console(config)#snmp-server view ifEntry.a 1.3.6.1.2.1.2.2.1.1.* included
Console(config)#
```

show snmp engine-id

This command shows the SNMP engine ID.

COMMAND MODE

Privileged Exec

EXAMPLE

This example shows the default engine ID.

```
Console#show snmp engine-id
Local SNMP EngineID: 8000002a8000000000e8666672
Local SNMP EngineBoots: 1

Remote SNMP EngineID                                    IP address
80000000030004e2b316c54321                              192.168.1.19
Console#
```

Table 55: show snmp engine-id - display description

Field	Description
Local SNMP engineID	String identifying the engine ID.
Local SNMP engineBoots	The number of times that the engine has (re-)initialized since the snmp EngineID was last configured.
Remote SNMP engineID	String identifying an engine ID on a remote device.
IP address	IP address of the device containing the corresponding remote SNMP engine.

show snmp group

Four default groups are provided – SNMPv1 read-only access and read/write access, and SNMPv2c read-only access and read/write access.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show snmp group
Group Name: r&d
Security Model: v3
Read View: defaultview
Write View: daily
Notify View: none
Storage Type: permanent
Row Status: active

Group Name: public
Security Model: v1
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: public
Security Model: v2c
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: private
Security Model: v1
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: private
Security Model: v2c
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

Console#
```

Table 56: show snmp group - display description

Field	Description
groupname	Name of an SNMP group.
security model	The SNMP version.
readview	The associated read view.
writeview	The associated write view.

Table 56: show snmp group - display description (Continued)

Field	Description
notifyview	The associated notify view.
storage-type	The storage type for this entry.
Row Status	The row status of this entry.

show snmp user

This command shows information on SNMP users.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show snmp user
EngineId: 800000ca030030f1df9ca00000
User Name: steve
Authentication Protocol: md5
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

SNMP remote user
EngineId: 80000000030004e2b316c54321
User Name: mark
Authentication Protocol: mdt
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

Console#
```

Table 57: show snmp user - display description

Field	Description
EngineId	String identifying the engine ID.
User Name	Name of user connecting to the SNMP agent.
Authentication Protocol	The authentication protocol used with SNMPv3.
Privacy Protocol	The privacy protocol used with SNMPv3.
Storage Type	The storage type for this entry.
Row Status	The row status of this entry.
SNMP remote user	A user associated with an SNMP engine on a remote device.

show snmp view

This command shows information on the SNMP views.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show snmp view
View Name: mib-2
Subtree OID: 1.2.2.3.6.2.1
View Type: included
Storage Type: permanent
Row Status: active

View Name: defaultview
Subtree OID: 1
View Type: included
Storage Type: volatile
Row Status: active

Console#
```

Table 58: show snmp view - display description

Field	Description
View Name	Name of an SNMP view.
Subtree OID	A branch in the MIB tree.
View Type	Indicates if the view is included or excluded.
Storage Type	The storage type for this entry.
Row Status	The row status of this entry.

snmp-server enable traps

This command enables this device to send Simple Network Management Protocol traps or informs (i.e., SNMP notifications). Use the **no** form to disable SNMP notifications.

SYNTAX

[**no**] **snmp-server enable traps** [**authentication** | **link-up-down** | **user-authentication authentication**]

authentication - Keyword to issue authentication failure notifications.

link-up-down - Keyword to issue link-up or link-down notifications.

user-authentication authentication - Keyword to issue user login authentication failure or success notifications. (Refer to the authentication login command.)

DEFAULT SETTING

Issue authentication, link-up-down, and user-authentication traps.

COMMAND MODE

Global Configuration

COMMAND USAGE

- If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order to configure

this device to send SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, both authentication and link-up-down notifications are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.

- The **snmp-server enable traps** command is used in conjunction with the snmp-server host command. Use the snmp-server host command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one snmp-server host command.
- The authentication, link-up, and link-down traps are legacy notifications, and therefore when used for SNMP Version 3 hosts, they must be enabled in conjunction with the corresponding entries in the Notify View assigned by the snmp-server group command.

EXAMPLE

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

RELATED COMMANDS

snmp-server host (540)

snmp-server host

This command specifies the recipient of a Simple Network Management Protocol notification operation. Use the **no** form to remove the specified host.

SYNTAX

snmp-server host *host-addr* [**inform** [**retry** *retries* | **timeout** *seconds*]] *community-string* [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} [**udp-port** *port*]}

no snmp-server host *host-addr*

host-addr - Internet address of the host (the targeted recipient). (Maximum host addresses: 5 trap destination IP address entries)

inform - Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)

retries - The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)

seconds - The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)

community-string - Password-like community string sent with the notification operation to SNMP V1 and V2c hosts. Although you can set this string using the **snmp-server host** command by itself, we

recommend defining it with the snmp-server community command prior to using the **snmp-server host** command. (Maximum length: 32 characters)

version - Specifies whether to send notifications as SNMP Version 1, 2c or 3 traps. (Range: 1, 2c, 3; Default: 1)

auth | **noauth** | **priv** - This group uses SNMPv3 with authentication, no authentication, or with authentication and privacy. See "Simple Network Management Protocol" for further information about these authentication and encryption options.

port - Host UDP port to use. (Range: 1-65535; Default: 162)

DEFAULT SETTING

Host Address: None
Notification Type: Traps
SNMP Version: 1
UDP Port: 162

COMMAND MODE

Global Configuration

COMMAND USAGE

- If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the switch to send SNMP notifications, you must enter at least one **snmp-server host** command. In order to enable multiple hosts, you must issue a separate **snmp-server host** command for each host.

- The **snmp-server host** command is used in conjunction with the snmp-server enable traps command. Use the snmp-server enable traps command to enable the sending of traps or informs and to specify which SNMP notifications are sent globally. For a host to receive notifications, at least one snmp-server enable traps command and the **snmp-server host** command for that host must be enabled.

- Some notification types cannot be controlled with the snmp-server enable traps command. For example, some notification types are always enabled.

- Notifications are issued by the switch as trap messages by default. The recipient of a trap message does not send a response to the switch. Traps are therefore not as reliable as inform messages, which include a request for acknowledgement of receipt. Informs can be used to ensure that critical information is received by the host. However, note that informs consume more system resources because they must be kept in memory until a response is received. Informs also add to network traffic. You should consider these effects when deciding whether to issue notifications as traps or informs.

To send an inform to a SNMPv2c host, complete these steps:

1. Enable the SNMP agent (page 528).
2. Create a view with the required notification messages (page 535).
3. Create a group that includes the required notify view (page 533).
4. Allow the switch to send SNMP traps; i.e., notifications (page 539).
5. Specify the target host that will receive inform messages with the **snmp-server host** command as described in this section.

To send an inform to a SNMPv3 host, complete these steps:

1. Enable the SNMP agent (page 528).
2. Create a local SNMPv3 user to use in the message exchange process (page 534).
3. Create a view with the required notification messages (page 535).
4. Create a group that includes the required notify view (page 533).
5. Allow the switch to send SNMP traps; i.e., notifications (page 539).
6. Specify the target host that will receive inform messages with the **snmp-server host** command as described in this section.

- The switch can send SNMP Version 1, 2c or 3 notifications to a host IP address, depending on the SNMP version that the management station supports. If the **snmp-server host** command does not specify the SNMP version, the default is to send SNMP version 1 notifications.

- If you specify an SNMP Version 3 host, then the community string is interpreted as an SNMP user name. The user name must first be defined with the snmp-server user command. Otherwise, an SNMPv3 group will be automatically created by the **snmp-server host** command using the name of the specified community string, and default settings for the read, write, and notify view.

EXAMPLE

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#
```

RELATED COMMANDS

snmp-server enable traps (539)

snmp-server enable traps mac-notification

This command globally enables the sending of trap messages when dynamic addresses are added to or removed from the MAC address table. Use the **no** form without any keywords to disable these traps. Use the **no** form with the **interval** keyword to restore the default collection interval.

SYNTAX

snmp-server enable traps mac-notification [**interval** *seconds*]

no snmp-server enable traps mac-notification [**interval**]

seconds - The delay between sending two consecutive trap messages. (Range: 0-3600 seconds)

DEFAULT SETTING
Disabled
1 second interval

COMMAND MODE
Global Configuration

COMMAND USAGE
- Dynamic entries stored in the address table are determined by examining the source address of ingress packets. This command is used to generate SNMP traps when a dynamic address is added to or removed from the MAC address table of an interface for which MAC notification traps have been enabled with the snmp-server enable port-traps mac-notification command.
- Changes to dynamic address entries in the MAC address table may occur due to address aging, changes in spanning tree topology, or for other reasons. Changes to static address entries are not included in this type of trap message.
- If the **interval** parameter is set to a non-zero value, trap messages will be stored in a buffer, and sent when the interval expires. The buffer can hold up to 512 messages. Note that some notifications may be lost if the buffer overflows during the specified interval.
- The attributes reported in these traps include the (1) MAC address, (2) VLAN identifier, (3) interface index, (4) and an ADD/REMOVE attribute indicating the type of change.

EXAMPLE
This example enables MAC notification traps, and sets the reporting interval to 10 seconds.

```
Console(config)#snmp-server enable traps mac-notification interval 10
Console(config)#
```

RELATED COMMANDS
show snmp (530)

snmp-server enable port-traps mac-notification

This command sends a trap when dynamic addresses are added to or removed from the MAC address table for an interface. Use the **no** form to disable these traps.

SYNTAX
[**no**] **snmp-server enable port-traps mac-notification**

DEFAULT SETTING
Disabled

COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE
MAC notification traps must also be globally enabled with the snmp-server enable traps mac-notification command for this interface-level command to take effect.

EXAMPLE
This example enables MAC notification traps on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps mac-notification
Console(config-if)#
```

show snmp-server enable port-traps interface

This command shows if trap messages will be sent when changes occur to dynamic entries in the MAC address table for an interface.

SYNTAX

show snmp-server enable port-traps interface [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE
Privileged Exec

EXAMPLE

```
Console#show snmp-server enable port-traps interface ethernet 1/1
Interface MAC Notification Trap
--------- --------------------
Eth 1/1                    Yes
Console#
```

23 FLOW SAMPLING COMMANDS

Flow sampling (sFlow) can be used with a remote sFlow Collector to provide an accurate, detailed and real-time overview of the types and levels of traffic present on the network. The sFlow Agent samples 1 out of *n* packets from all data traversing the switch, re-encapsulates the samples as sFlow datagrams and transmits them to the sFlow Collector. This sampling occurs at the internal hardware level where all traffic is seen, whereas traditional probes only have a partial view of traffic as it is sampled at the monitored interface. Moreover, the processor and memory load imposed by the sFlow agent is minimal since local analysis does not take place.

Table 59: sFlow Commands

Command	Function	Mode
sflow	Enables sFlow globally for the switch	GC
sflow source*	Enables sFlow on the source ports to be monitored	IC
sflow sample*	Configures the packet sampling rate	IC
sflow polling-interval	Configures the interval at which counters are added to the sample datagram	IC
sflow owner	Configures the name of the receiver	IC
sflow timeout	Configures the length of time samples are sent to the Collector before resetting all sFlow port parameters	IC
sflow destination	Configures the IP address and UDP port used by the Collector	IC
sflow max-header-size	Configures the maximum size of the sFlow datagram header	IC
sflow max-datagram-size	Configures the maximum size of the sFlow datagram payload	IC
show sflow	Shows the global and interface settings for the sFlow process	PE

* Due to the switch's hardware design, these commands can only be enabled for specific port groups (1-8, 9-16, 17-24, 25-32, 33-48). However, sampling for each of the Gigabit combination ports (25-28/49-52) can be controlled individually.

sflow

This command enables sFlow globally for the switch. Use the **no** form to disable this feature.

SYNTAX

[**no**] **sflow**

DEFAULT SETTING

Disabled

COMMAND MODE
Global Configuration

COMMAND USAGE
Flow sampling must be enabled globally on the switch, as well as for those ports where it is required (see the sflow source command).

EXAMPLE

```
Console(config)#sflow
Console(config)#
```

sflow source

This command enables sFlow on the source ports to be monitored. Use the **no** form to disable sFlow on the specified ports.

SYNTAX

[**no**] **sflow source**

DEFAULT SETTING
Disabled

COMMAND MODE
Interface Configuration (Ethernet)

COMMAND USAGE
The 100BASE-TX ports are organized into groups of 8 based on a restriction in the switch ASIC (1-8, 9-16, 17-24, 25-32, 33-48). Selecting any port in one of these groups effectively configures all of the group members as an sFlow source port. However, the four Gigabit ports (25-28/49-52) can be independently configured as an sFlow source port.

EXAMPLE
This example enables flow control on ports 9 through 16.

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow source
Console(config-if)#
```

sflow sample

This command configures the packet sampling rate. Use the **no** form to restore the default rate.

SYNTAX

sflow sample *rate*

no sflow sample

rate - The packet sampling rate, or the number of packets out of which one sample will be taken. (Range: 0-10000000, where 0 disables sampling)

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

This example sets the sample rate to 1 out of every 100 packets.

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow sample 100
Console(config-if)#
```

sflow polling-interval

This command configures the interval at which counters are added to the sample datagram. Use the **no** form to restore the default polling interval.

SYNTAX

sflow polling-interval *seconds*

no sflow polling-interval

seconds - The interval at which the sFlow process adds counter values to the sample datagram. (Range: 0-10000000 seconds, where 0 disables this feature)

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

This example sets the polling interval to 10 seconds.

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow polling-interval 10
Console(config-if)#
```

sflow owner

This command configures the name of the receiver (i.e., sFlow Collector). Use the **no** form to remove this name.

SYNTAX

sflow owner *name*

no sflow owner

name - The name of the receiver. (Range: 1-256 characters)

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

This example set the owner's name to Lamar.

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow owner Lamer
Console(config-if)#
```

sflow timeout

This command configures the length of time samples are sent to the Collector before resetting all sFlow port parameters. Use the **no** form to restore the default time out.

SYNTAX

sflow timeout *seconds*

no sflow timeout

seconds - The length of time the sFlow process continuously sends samples to the Collector before resetting all sFlow port parameters. (Range: 0-10000000 seconds, where 0 indicates no time out)

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

The sFlow parameters affected by this command include the sampling interval, the receiver's name, address and UDP port, the time out, maximum header size, and maximum datagram size.

EXAMPLE

This example sets the time out to 1000 seconds.

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow timeout 10000
Console(config-if)#
```

sflow destination

This command configures the IP address and UDP port used by the Collector. Use the **no** form to restore the default settings.

SYNTAX

sflow destination ipv4 *ip-address* [*destination-udp-port*]

no sflow destination

ip-address - IP address of the sFlow Collector.

destination-udp-port - The UDP port on which the Collector is listening for sFlow streams. (Range: 0-65534)

DEFAULT SETTING

IP Address: null
UDP Port: 6343

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

This example configures the Collector's IP address, and uses the default UDP port.

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow destination ipv4 192.168.0.4
Console(config-if)#
```

sflow max-header-size

This command configures the maximum size of the sFlow datagram header. Use the **no** form to restore the default setting.

SYNTAX

sflow max-header-size *max-header-size*

no max-header-size

max-header-size - The maximum size of the sFlow datagram header. (Range: 64-256 bytes)

DEFAULT SETTING

128 bytes

COMMAND MODE
Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow max-header-size 256
Console(config-if)#
```

sflow max-datagram-size

This command configures the maximum size of the sFlow datagram payload. Use the **no** form to restore the default setting.

SYNTAX

sflow max-datagram-size *max-datagram-size*

no max-datagram-size

max-datagram-size - The maximum size of the sFlow datagram payload. (Range: 200-1500 bytes)

DEFAULT SETTING
1400 bytes

COMMAND MODE
Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow max-datagram-size 1500
Console(config-if)#
```

show sflow

This command shows the global and interface settings for the sFlow process.

SYNTAX

show sflow [**interface** [*interface*]]

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28/52)

COMMAND MODE
Privileged Exec

EXAMPLE

```
Console#show sflow

 sFlow global status : Enabled

Console#sh sf int e 1/9

 Interface of Ethernet  1/9  :
   Interface status      : Enabled
   Owner name            : Lamar
   Owner destination     : 192.168.0.4
   Owner socket port     : 6343
   Time out              : 10000
   Maximum header size   : 256
   Maximum datagram size : 1500
   Sample rate           : 1/100
   Polling interval      : 10

Console#
```

24 AUTHENTICATION COMMANDS

You can configure this switch to authenticate users logging into the system for management access using local or remote authentication methods. Port-based authentication using IEEE 802.1X can also be configured to control either management access to the uplink ports or client access[16] to the data ports.

Table 60: Authentication Commands

Command Group	Function
User Accounts	Configures the basic user names and passwords for management access
Authentication Sequence	Defines logon authentication method and precedence
RADIUS Client	Configures settings for authentication via a RADIUS server
TACACS+ Client	Configures settings for authentication via a TACACS+ server
AAA	Configures authentication, authorization, and accounting for network access
Web Server	Enables management access via a web browser
Telnet Server	Enables management access via Telnet
Secure Shell	Provides secure replacement for Telnet
802.1X Port Authentication	Configures host authentication on specific ports using 802.1X
Management IP Filter	Configures IP addresses that are allowed management access
PPPoE Intermediate Agent	Configures relay parameters required for sending authentication messages between a client and broadband remote access servers

16. For other methods of controlling client access, see "General Security Measures."

USER ACCOUNTS

The basic commands required for management access are listed in this section. This switch also includes other options for password checking via the console or a Telnet connection (page 481), user authentication via a remote authentication server (page 553), and host access authentication for specific ports (page 590).

Table 61: User Access Commands

Command	Function	Mode
enable password	Sets a password to control access to the Privileged Exec level	GC
username	Establishes a user name-based authentication system at login	GC

enable password

After initially logging onto the system, you should set the Privileged Exec password. Remember to record it in a safe place. This command controls access to the Privileged Exec level from the Normal Exec level. Use the **no** form to reset the default password.

SYNTAX

enable password [**level** *level*] {**0** | **7**} *password*

no enable password [**level** *level*]

level *level* - Level 15 for Privileged Exec. (Levels 0-14 are not used.)

{**0** | **7**} - 0 means plain password, 7 means encrypted password.

password - password for this privilege level. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

DEFAULT SETTING

The default is level 15.
The default password is "super"

COMMAND MODE

Global Configuration

COMMAND USAGE

- You cannot set a null password. You will have to enter a password to change the command mode from Normal Exec to Privileged Exec with the enable command.

- The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

EXAMPLE

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

RELATED COMMANDS

enable (447)
authentication enable (556)

username

This command adds named users, requires authentication at login, specifies or changes a user's password (or specify that no password is required), or specifies or changes a user's access level. Use the **no** form to remove a user name.

SYNTAX

username *name* {**access-level** *level* | **nopassword** | **password** {**0** | **7**} *password*}

no username *name*

name - The name of the user. (Maximum length: 8 characters, case sensitive. Maximum users: 16)

access-level *level* - Specifies the user level.
The device has two predefined privilege levels:
0: Normal Exec, **15**: Privileged Exec.

nopassword - No password is required for this user to log in.

{**0** | **7**} - 0 means plain password, 7 means encrypted password.

password *password* - The authentication password for the user. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

DEFAULT SETTING

The default access level is Normal Exec.
The factory defaults for the user names and passwords are:

Table 62: Default Login Settings

username	access-level	password
guest	0	guest
admin	15	admin

COMMAND MODE

Global Configuration

COMMAND USAGE

The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

EXAMPLE

This example shows how the set the access level and password for a user.

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

AUTHENTICATION SEQUENCE

Three authentication methods can be specified to authenticate users logging into the system for management access. The commands in this section can be used to define the authentication method and sequence.

Table 63: Authentication Sequence Commands

Command	Function	Mode
authentication enable	Defines the authentication method and precedence for command mode change	GC
authentication login	Defines logon authentication method and precedence	GC

authentication enable

This command defines the authentication method and precedence to use when changing from Exec command mode to Privileged Exec command mode with the enable command. Use the **no** form to restore the default.

SYNTAX

authentication enable {[**local**] [**radius**] [**tacacs**]}

no authentication enable

local - Use local password only.

radius - Use RADIUS server password only.

tacacs - Use TACACS server password.

DEFAULT SETTING

Local

COMMAND MODE

Global Configuration

COMMAND USAGE

- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.

- RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter "**authentication enable radius tacacs local**," the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

EXAMPLE

```
Console(config)#authentication enable radius
Console(config)#
```

RELATED COMMANDS

enable password - sets the password for changing command modes (554)

authentication login

This command defines the login authentication method and precedence. Use the **no** form to restore the default.

SYNTAX

authentication login {[**local**] [**radius**] [**tacacs**]}

no authentication login

local - Use local password.

radius - Use RADIUS server password.

tacacs - Use TACACS server password.

DEFAULT SETTING

Local

COMMAND MODE

Global Configuration

COMMAND USAGE

- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.
- RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter

"**authentication login radius tacacs local**," the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

EXAMPLE

```
Console(config)#authentication login radius
Console(config)#
```

RELATED COMMANDS

username - for setting the local user names and passwords (555)

RADIUS CLIENT

Remote Authentication Dial-in User Service (RADIUS) is a logon authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Table 64: RADIUS Client Commands

Command	Function	Mode
radius-server acct-port	Sets the RADIUS server network port	GC
radius-server auth-port	Sets the RADIUS server network port	GC
radius-server host	Specifies the RADIUS server	GC
radius-server key	Sets the RADIUS encryption key	GC
radius-server retransmit	Sets the number of retries	GC
radius-server timeout	Sets the interval between sending authentication requests	GC
show radius-server	Shows the current RADIUS settings	PE

radius-server acct-port

This command sets the RADIUS server network port for accounting messages. Use the **no** form to restore the default.

SYNTAX

radius-server acct-port *port-number*

no radius-server acct-port

port-number - RADIUS server UDP port used for accounting messages. (Range: 1-65535)

DEFAULT SETTING

1813

COMMAND MODE
Global Configuration

EXAMPLE

```
Console(config)#radius-server acct-port 181
Console(config)#
```

radius-server auth-port

This command sets the RADIUS server network port. Use the **no** form to restore the default.

SYNTAX

radius-server auth-port *port-number*

no radius-server auth-port

port-number - RADIUS server UDP port used for authentication messages. (Range: 1-65535)

DEFAULT SETTING
1812

COMMAND MODE
Global Configuration

EXAMPLE

```
Console(config)#radius-server auth-port 181
Console(config)#
```

radius-server host

This command specifies primary and backup RADIUS servers, and authentication and accounting parameters that apply to each server. Use the **no** form to remove a specified server, or to restore the default values.

SYNTAX

[**no**] **radius-server** *index* **host** *host-ip-address* [**auth-port** *auth-port*] [**acct-port** *acct-port*] [**key** *key*] [**retransmit** *retransmit*] [**timeout** *timeout*]

index - Allows you to specify up to five servers. These servers are queried in sequence until a server responds or the retransmit period expires.

host-ip-address - IP address of server.

auth-port - RADIUS server UDP port used for authentication messages. (Range: 1-65535)

acct-port - RADIUS server UDP port used for accounting messages. (Range: 1-65535)

key - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)

retransmit - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1-30)

timeout - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

DEFAULT SETTING

auth-port - 1812
acct-port - 1813
timeout - 5 seconds
retransmit - 2

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#radius-server 1 host 192.168.1.20 port 181 timeout 10
  retransmit 5 key green
Console(config)#
```

radius-server key

This command sets the RADIUS encryption key. Use the **no** form to restore the default.

SYNTAX

radius-server key *key-string*

no radius-server key

key-string - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#radius-server key green
Console(config)#
```

radius-server retransmit

This command sets the number of retries. Use the **no** form to restore the default.

SYNTAX

radius-server retransmit *number-of-retries*

no radius-server retransmit

number-of-retries - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1 - 30)

DEFAULT SETTING

2

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#radius-server retransmit 5
Console(config)#
```

radius-server timeout

This command sets the interval between transmitting authentication requests to the RADIUS server. Use the **no** form to restore the default.

SYNTAX

radius-server timeout *number-of-seconds*

no radius-server timeout

number-of-seconds - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

DEFAULT SETTING

5

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#radius-server timeout 10
Console(config)#
```

show radius-server

This command displays the current settings for the RADIUS server.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show radius-server

Remote RADIUS Server Configuration:

Global Settings:
 Authentication Port:                  1812
 Accounting Port:                      1813
 Retransmit Times:                     2
 Request Timeout:                      5

Server 1:
 Server IP Address:                    192.168.1.1
 Authentication Port:                  1812
 Accounting Port:                      1813
 Retransmit Times:                     2
 Request Timeout:                      5

Radius server group:
Group Name                Member Index
--------------------      -------------
radius                           1

Console#
```

TACACS+ CLIENT

Terminal Access Controller Access Control System (TACACS+) is a logon authentication protocol that uses software running on a central server to control access to TACACS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Table 65: TACACS+ Client Commands

Command	Function	Mode
tacacs-server	Specifies the TACACS+ server and optional parameters	GC
tacacs-server host	Specifies the TACACS+ server	GC
tacacs-server key	Sets the TACACS+ encryption key	GC
tacacs-server port	Specifies the TACACS+ server network port	GC
tacacs-server retransmit	Sets the number of retries	GC

Table 65: TACACS+ Client Commands (Continued)

Command	Function	Mode
tacacs-server timeout	Sets the interval before resending an authentication request	GC
show tacacs-server	Shows the current TACACS+ settings	GC

tacacs-server

This command specifies the TACACS+ server and other optional parameters. Use the **no** form to remove the server, or to restore the default values.

SYNTAX

tacacs-server *index* **host** *host-ip-address* [**key** *key*] [**port** *port-number*]

no tacacs-server *index*

index - The index for this server. (Range: 1)

host-ip-address - IP address of a TACACS+ server.

key - Encryption key used to authenticate logon access for the client. Do not use blank spaces in the string. (Maximum length: 48 characters)

port-number - TACACS+ server TCP port used for authentication messages. (Range: 1-65535)

DEFAULT SETTING

10.11.12.13

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#tacacs-server host 192.168.1.25
Console(config)#
```

tacacs-server host

This command specifies the TACACS+ server. Use the **no** form to restore the default.

SYNTAX

tacacs-server host *host-ip-address*

no tacacs-server host

host-ip-address - IP address of a TACACS+ server.

DEFAULT SETTING

10.11.12.13

COMMAND MODE
Global Configuration

EXAMPLE

```
Console(config)#tacacs-server host 192.168.1.25
Console(config)#
```

tacacs-server key

This command sets the TACACS+ encryption key. Use the **no** form to restore the default.

SYNTAX

tacacs-server key *key-string*

no tacacs-server key

key-string - Encryption key used to authenticate logon access for the client. Do not use blank spaces in the string. (Maximum length: 48 characters)

DEFAULT SETTING
None

COMMAND MODE
Global Configuration

EXAMPLE

```
Console(config)#tacacs-server key green
Console(config)#
```

tacacs-server port

This command specifies the TACACS+ server network port. Use the **no** form to restore the default.

SYNTAX

tacacs-server port *port-number*

no tacacs-server port

port-number - TACACS+ server TCP port used for authentication messages. (Range: 1-65535)

DEFAULT SETTING
49

COMMAND MODE
Global Configuration

EXAMPLE

```
Console(config)#tacacs-server port 181
Console(config)#
```

tacacs-server retransmit

This command sets the number of retries. Use the **no** form to restore the default.

SYNTAX

tacacs-server retransmit *number-of-retries*

no tacacs-server retransmit

number-of-retries - Number of times the switch will try to authenticate logon access via the TACACS+ server. (Range: 1-30)

DEFAULT SETTING

2

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#tacacs-server retransmit 5
Console(config)#
```

tacacs-server timeout

This command sets the interval between transmitting authentication requests to the TACACS+ server. Use the **no** form to restore the default.

SYNTAX

tacacs-server timeout *number-of-seconds*

no tacacs-server timeout

number-of-seconds - Number of seconds the switch waits for a reply before resending a request. (Range: 1-540)

DEFAULT SETTING

5 seconds

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#tacacs-server timeout 10
Console(config)#
```

show tacacs-server

This command displays the current settings for the TACACS+ server.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show tacacs-server

Remote TACACS+ server configuration:

Global Settings:
 Server Port Number:                    49
 Retransmit Times  :                    2
 Request Times     :                    5

Server 1:
 Server IP address:                     1.2.3.4
 Server port number:                    49
 Retransmit Times  :                    2
 Request Times     :                    5

Tacacs server group:
Group Name                 Member Index
---------------------      -------------
tacacs+                           1

Console#
```

AAA

The Authentication, Authorization, and Accounting (AAA) feature provides the main framework for configuring access control on the switch. The AAA functions require the use of configured RADIUS or TACACS+ servers in the network.

Table 66: AAA Commands

Command	Function	Mode
aaa accounting commands	Enables accounting of Exec mode commands	GC
aaa accounting dot1x	Enables accounting of 802.1X services	GC
aaa accounting exec	Enables accounting of Exec services	GC
aaa accounting update	Enables periodoc updates to be sent to the accounting server	GC
aaa authorization exec	Enables authorization of Exec sessions	GC
aaa group server	Groups security servers in to defined lists	GC
server	Configures the IP address of a server in a group list	SG

Table 66: AAA Commands (Continued)

Command	Function	Mode
accounting dot1x	Applies an accounting method to an interface for 802.1X service requests	IC
accounting commands	Applies an accounting method to CLI commands entered by a user	Line
accounting exec	Applies an accounting method to local console, Telnet or SSH connections	Line
authorization exec	Applies an authorization method to local console, Telnet or SSH connections	Line
show accounting	Displays all accounting information	PE

aaa accounting commands

This command enables the accounting of Exec mode commands. Use the **no** form to disable the accounting service.

SYNTAX

aaa accounting commands *level* {**default** | *method-name*}
start-stop group {**tacacs+** |*server-group*}

no aaa accounting commands *level* {**default** | *method-name*}

level - The privilege level for executing commands. (Range: 0-15)

default - Specifies the default accounting method for service requests.

method-name - Specifies an accounting method for service requests. (Range: 1-255 characters)

start-stop - Records accounting from starting point and stopping point.

group - Specifies the server group to use.

tacacs+ - Specifies all TACACS+ hosts configure with the tacacs-server host command.

server-group - Specifies the name of a server group configured with the aaa group server command. (Range: 1-255 characters)

DEFAULT SETTING

Accounting is not enabled
No servers are specified

COMMAND MODE

Global Configuration

COMMAND USAGE

- The accounting of Exec mode commands is only supported by TACACS+ servers.
- Note that the **default** and *method-name* fields are only used to describe the accounting method(s) configured on the specified

TACACS+ server, and do not actually send any information to the server about the methods to use.

EXAMPLE

```
Console(config)#aaa accounting commands 15 default start-stop group tacacs+
Console(config)#
```

aaa accounting dot1x

This command enables the accounting of requested 802.1X services for network access. Use the **no** form to disable the accounting service.

SYNTAX

aaa accounting dot1x {**default** | *method-name*}
start-stop group {**radius** | **tacacs+** |*server-group*}

no aaa accounting dot1x {**default** | *method-name*}

default - Specifies the default accounting method for service requests.

method-name - Specifies an accounting method for service requests. (Range: 1-255 characters)

start-stop - Records accounting from starting point and stopping point.

group - Specifies the server group to use.

radius - Specifies all RADIUS hosts configure with the radius-server host command.

tacacs+ - Specifies all TACACS+ hosts configure with the tacacs-server host command.

server-group - Specifies the name of a server group configured with the aaa group server command. (Range: 1-255 characters)

DEFAULT SETTING

Accounting is not enabled
No servers are specified

COMMAND MODE

Global Configuration

COMMAND USAGE

Note that the **default** and *method-name* fields are only used to describe the accounting method(s) configured on the specified RADIUS or TACACS+ servers, and do not actually send any information to the servers about the methods to use.

EXAMPLE

```
Console(config)#aaa accounting dot1x default start-stop group radius
Console(config)#
```

aaa accounting exec

This command enables the accounting of requested Exec services for network access. Use the **no** form to disable the accounting service.

SYNTAX

aaa accounting exec {**default** | *method-name*}
start-stop group {**radius** | **tacacs+** |*server-group*}

no aaa accounting exec {**default** | *method-name*}

default - Specifies the default accounting method for service requests.

method-name - Specifies an accounting method for service requests. (Range: 1-255 characters)

start-stop - Records accounting from starting point and stopping point.

group - Specifies the server group to use.

radius - Specifies all RADIUS hosts configure with the radius-server host command.

tacacs+ - Specifies all TACACS+ hosts configure with the tacacs-server host command.

server-group - Specifies the name of a server group configured with the aaa group server command. (Range: 1-255 characters)

DEFAULT SETTING

Accounting is not enabled
No servers are specified

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command runs accounting for Exec service requests for the local console and Telnet connections.
- Note that the **default** and *method-name* fields are only used to describe the accounting method(s) configured on the specified RADIUS or TACACS+ servers, and do not actually send any information to the servers about the methods to use.

EXAMPLE

```
Console(config)#aaa accounting exec default start-stop group tacacs+
Console(config)#
```

aaa accounting update

This command enables the sending of periodic updates to the accounting server. Use the **no** form to disable accounting updates.

SYNTAX

aaa accounting update [**periodic** *interval*]

no aaa accounting update

interval - Sends an interim accounting record to the server at this interval. (Range: 1-2147483647 minutes)

DEFAULT SETTING

1 minute

COMMAND MODE

Global Configuration

COMMAND USAGE

- When accounting updates are enabled, the switch issues periodic interim accounting records for all users on the system.
- Using the command without specifying an interim interval enables updates, but does not change the current interval setting.

EXAMPLE

```
Console(config)#aaa accounting update periodic 30
Console(config)#
```

aaa authorization exec

This command enables the authorization for Exec access. Use the **no** form to disable the authorization service.

SYNTAX

aaa authorization exec {**default** | *method-name*}
group {**tacacs+** | *server-group*}

no aaa authorization exec {**default** | *method-name*}

default - Specifies the default authorization method for Exec access.

method-name - Specifies an authorization method for Exec access. (Range: 1-255 characters)

group - Specifies the server group to use.

tacacs+ - Specifies all TACACS+ hosts configured with the tacacs-server command.

server-group - Specifies the name of a server group configured with the aaa group server command. (Range: 1-255 characters)

DEFAULT SETTING
Authorization is not enabled
No servers are specified

COMMAND MODE
Global Configuration

COMMAND USAGE
- This command performs authorization to determine if a user is allowed to run an Exec shell.
- AAA authentication must be enabled before authorization is enabled.
- If this command is issued without a specified named method, the default method list is applied to all interfaces or lines (where this authorization type applies), except those that have a named method explicitly defined.

EXAMPLE
```
Console(config)#aaa authorization exec default group tacacs+
Console(config)#
```

aaa group server

Use this command to name a group of security server hosts. To remove a server group from the configuration list, enter the **no** form of this command.

SYNTAX
[**no**] **aaa group server** {**radius** | **tacacs+**} *group-name*

radius - Defines a RADIUS server group.

tacacs+ - Defines a TACACS+ server group.

group-name - A text string that names a security server group. (Range: 1-7 characters)

DEFAULT SETTING
None

COMMAND MODE
Global Configuration

EXAMPLE
```
Console(config)#aaa group server radius tps
Console(config-sg-radius)#
```

server

This command adds a security server to an AAA server group. Use the **no** form to remove the associated server from the group.

SYNTAX

[**no**] **server** {*index* | *ip-address*}

index - Specifies the server index.
(Range: RADIUS 1-5, TACACS+ 1)

ip-address - Specifies the host IP address of a server.

DEFAULT SETTING

None

COMMAND MODE

Server Group Configuration

COMMAND USAGE

- When specifying the index for a RADIUS server, that server index must already be defined by the radius-server host command.
- When specifying the index for a TACACS+ server, that server index must already be defined by the tacacs-server host command.

EXAMPLE

```
Console(config)#aaa group server radius tps
Console(config-sg-radius)#server 10.2.68.120
Console(config-sg-radius)#
```

accounting dot1x

This command applies an accounting method for 802.1X service requests on an interface. Use the **no** form to disable accounting on the interface.

SYNTAX

accounting dot1x {**default** | *list-name*}

no accounting dot1x

default - Specifies the default method list created with the aaa accounting dot1x command.

list-name - Specifies a method list created with the aaa accounting dot1x command.

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration

EXAMPLE

```
Console(config)#interface ethernet 1/2
Console(config-if)#accounting dot1x tps
Console(config-if)#
```

accounting commands

This command applies an accounting method to entered CLI commands. Use the **no** form to disable accounting for entered CLI commands.

SYNTAX

accounting commands *level* {**default** | *list-name*}

no accounting commands *level*

level - The privilege level for executing commands. (Range: 0-15)

default - Specifies the default method list created with the aaa accounting commands command.

list-name - Specifies a method list created with the aaa accounting commands command.

DEFAULT SETTING

None

COMMAND MODE

Line Configuration

EXAMPLE

```
Console(config)#line console
Console(config-line)#accounting commands 15 default
Console(config-line)#
```

accounting exec

This command applies an accounting method to local console or Telnet connections. Use the **no** form to disable accounting on the line.

SYNTAX

accounting exec {**default** | *list-name*}

no accounting exec

default - Specifies the default method list created with the aaa accounting exec command.

list-name - Specifies a method list created with the aaa accounting exec command.

DEFAULT SETTING

None

COMMAND MODE
Line Configuration

EXAMPLE

```
Console(config)#line console
Console(config-line)#accounting exec tps
Console(config-line)#exit
Console(config)#line vty
Console(config-line)#accounting exec default
Console(config-line)#
```

authorization exec

This command applies an authorization method to local console or Telnet connections. Use the **no** form to disable authorization on the line.

SYNTAX

authorization exec {**default** | *list-name*}
no authorization exec

default - Specifies the default method list created with the aaa authorization exec command.

list-name - Specifies a method list created with the aaa authorization exec command.

DEFAULT SETTING
None

COMMAND MODE
Line Configuration

EXAMPLE

```
Console(config)#line console
Console(config-line)#authorization exec tps
Console(config-line)#exit
Console(config)#line vty
Console(config-line)#authorization exec default
Console(config-line)#
```

show accounting

This command displays the current accounting settings per function and per port.

SYNTAX

show accounting [**commands** [*level*]] |
[[**dot1x** [**statistics** [**username** *user-name* | **interface** *interface*]] | **exec** [**statistics**] | **statistics**]

commands - Displays command accounting information.

level - Displays command accounting information for a specifiable command level.

dot1x - Displays dot1x accounting information.

exec - Displays Exec accounting records.

statistics - Displays accounting records.

user-name - Displays accounting records for a specifiable username.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show accounting
Accounting type: dot1x
  Method list: default
  Group list: radius
  Interface:

  Method list: tps
  Group list: radius
  Interface: eth 1/2

Accounting type: Exec
  Method list: default
  Group list: radius
  Interface: vty

Console#
```

WEB SERVER

This section describes commands used to configure web browser management access to the switch.

Table 67: Web Server Commands

Command	Function	Mode
ip http port	Specifies the port to be used by the web browser interface	GC
ip http secure-port	Specifies the UDP port number for HTTPS	GC
ip http secure-server	Enables HTTPS (HTTP/SSL) for encrypted communications	GC
ip http server	Allows the switch to be monitored or configured from a browser	GC

ip http port

This command specifies the TCP port number used by the web browser interface. Use the **no** form to use the default port.

SYNTAX

ip http port *port-number*

no ip http port

port-number - The TCP port to be used by the browser interface. (Range: 1-65535)

DEFAULT SETTING

80

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#ip http port 769
Console(config)#
```

RELATED COMMANDS

ip http server (579)
show system (467)

ip http secure-port

This command specifies the UDP port number used for HTTPS connection to the switch's web interface. Use the **no** form to restore the default port.

SYNTAX

ip http secure-port *port-number*

no ip http secure-port

port-number – The UDP port used for HTTPS. (Range: 1-65535)

DEFAULT SETTING

443

COMMAND MODE

Global Configuration

COMMAND USAGE

- You cannot configure the HTTP and HTTPS servers to use the same port.
- If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format: **https://***device***:***port-number*

EXAMPLE

```
Console(config)#ip http secure-port 1000
Console(config)#
```

RELATED COMMANDS

ip http secure-server (577)
show system (467)

ip http secure-server

This command enables the secure hypertext transfer protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's web interface. Use the **no** form to disable this function.

SYNTAX

[**no**] **ip http secure-server**

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- Both HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure the HTTP and HTTPS servers to use the same UDP port.
- If you enable HTTPS, you must indicate this in the URL that you specify in your browser: **https**://*device*[:*port-number*]
- When you start HTTPS, the connection is established in this way:
  - The client authenticates the server using the server's digital certificate.
  - The client and server negotiate a set of security protocols to use for the connection.
  - The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection.

  A padlock icon should appear in the status bar for Internet Explorer 5.x or above, Netscape Navigator 6.2 or above, and Mozilla Firefox 2.0.0.0 or above.

  The following web browsers and operating systems currently support HTTPS:

Table 68: HTTPS System Support

Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Windows Vista, Windows 7
Netscape Navigator 6.2 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6
Mozilla Firefox 2.0.0.0 or later	Windows 2000, Windows XP, Linux

- To specify a secure-site certificate, see "Replacing the Default Secure-site Certificate." Also refer to the copy tftp https-certificate command.

EXAMPLE

```
Console(config)#ip http secure-server
Console(config)#
```

RELATED COMMANDS

ip http secure-port (577)
copy tftp https-certificate (473)
show system (467)

ip http server

This command allows this device to be monitored or configured from a browser. Use the **no** form to disable this function.

SYNTAX

[**no**] **ip http server**

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#ip http server
Console(config)#
```

RELATED COMMANDS

ip http port (576)
show system (467)

TELNET SERVER

This section describes commands used to configure Telnet management access to the switch.

Table 69: Telnet Server Commands

Command	Function	Mode
ip telnet server	Allows the switch to be monitored or configured from Telnet; also specifies the port to be used by the Telnet interface	GC

NOTE: This switch also supports a Telnet client function. A Telnet connection can be made from this switch to another device by entering the **telnet** command at the Privileged Exec configuration level.

ip telnet server

This command allows this device to be monitored or configured from Telnet. It also specifies the TCP port number used by the Telnet interface. Use the **no** form without the "port" keyword to disable this function. Use the **no** from with the "port" keyword to use the default port.

SYNTAX

ip telnet server [**port** *port-number*]

no ip telnet server [**port**]

port - The TCP port used by the Telnet interface.

port-number - The TCP port number to be used by the browser interface. (Range: 1-65535)

DEFAULT SETTING

Enabled
TCP Port 23

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#ip telnet server
Console(config)#ip telnet server port 123
Console(config)#
```

SECURE SHELL

This section describes the commands used to configure the SSH server. Note that you also need to install a SSH client on the management station when using this protocol to configure the switch.

NOTE: The switch supports both SSH Version 1.5 and 2.0 clients.

Table 70: Secure Shell Commands

Command	Function	Mode
ip ssh authentication-retries	Specifies the number of retries allowed by a client	GC
ip ssh server	Enables the SSH server on the switch	GC
ip ssh server-key size	Sets the SSH server key size	GC
ip ssh timeout	Specifies the authentication timeout for the SSH server	GC
copy ftp public-key	Copies the user's public key from an FTP server to the switch	PE

Table 70: Secure Shell Commands (Continued)

Command	Function	Mode
copy tftp public-key	Copies the user's public key from a TFTP server to the switch	PE
delete public-key	Deletes the public key for the specified user	PE
disconnect	Terminates a line connection	PE
ip ssh crypto host-key generate	Generates the host key	PE
ip ssh crypto zeroize	Clear the host key from RAM	PE
ip ssh save host-key	Saves the host key from RAM to flash memory	PE
show ip ssh	Displays the status of the SSH server and the configured values for authentication timeout and retries	PE
show public-key	Shows the public key for the specified user or for the host	PE
show ssh	Displays the status of current SSH sessions	PE
show users	Shows SSH users, including privilege level and public key type	PE

Configuration Guidelines

The SSH server on this switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified by the authentication login command. If public key authentication is specified by the client, then you must configure authentication keys on both the client and the switch as described in the following section. Note that regardless of whether you use public key or password authentication, you still have to generate authentication keys on the switch and enable the SSH server.

To use the SSH server, complete these steps:

1. Generate a Host Key Pair – Use the ip ssh crypto host-key generate command to create a host public/private key pair.

2. Provide Host Public Key to Clients – Many SSH client programs automatically import the host public key during the initial connection setup with the switch. Otherwise, you need to manually create a known hosts file on the management station and place the host public key in it. An entry for a public key in the known hosts file would appear similar to the following example:

   10.1.0.54 1024 35
   15684995401867669259333946775054617325313674890836547254
   15020245593199868544358361651999923329781766065830956
   10825913212890233765468017262725714134287629413011961955667825
   95664104869574278881462065194174677298486546861571773939016477
   93559423035774130980227370877945452408397175264635805817671670
   9574804776117

3. Import Client's Public Key to the Switch – Use the copy tftp public-key command to copy a file containing the public key for all the SSH client's granted management access to the switch. (Note that these clients must be configured locally on the switch with the username command.) The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as shown in the following example for an RSA key:

   1024 35
   134108168560989392104094492015542534763164192187295892114317380055536161631051775940838686311092912322268285192543746031009371877211996963178136627741416898513204911720483033925432410163799759237144901193800609025394840848271781943722884025331159521348610229029789827213532671316294325328189150453063939166430steve@192.168.1.19

4. Set the Optional Parameters – Set other optional parameters, including the authentication timeout, the number of retries, and the server key size.

5. Enable SSH Service – Use the ip ssh server command to enable the SSH server on the switch.

6. *Authentication* – One of the following authentication methods is employed:

   Password Authentication (for SSH v1.5 or V2 Clients)

   a. The client sends its password to the server.
   b. The switch compares the client's password to those stored in memory.
   c. If a match is found, the connection is allowed.

NOTE: To use SSH with only password authentication, the host public key must still be given to the client, either during initial connection or manually entered into the known host file. However, you do not need to configure the client's keys.

   Public Key Authentication – When an SSH client attempts to contact the switch, the SSH server uses the host key pair to negotiate a session key and encryption method. Only clients that have a private key corresponding to the public keys stored on the switch can access it. The following exchanges take place during this process:

   Authenticating SSH v1.5 Clients

   a. The client sends its RSA public key to the switch.
   b. The switch compares the client's public key to those stored in memory.
   c. If a match is found, the switch uses its secret key to generate a random 256-bit string as a challenge, encrypts this string with the user's public key, and sends it to the client.

d. The client uses its private key to decrypt the challenge string, computes the MD5 checksum, and sends the checksum back to the switch.
e. The switch compares the checksum sent from the client against that computed for the original string it sent. If the two checksums match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

Authenticating SSH v2 Clients

a. The client first queries the switch to determine if DSA public key authentication using a preferred algorithm is acceptable.
b. If the specified algorithm is supported by the switch, it notifies the client to proceed with the authentication process. Otherwise, it rejects the request.
c. The client sends a signature generated using the private key to the switch.
d. When the server receives this message, it checks whether the supplied key is acceptable for authentication, and if so, it then checks whether the signature is correct. If both checks succeed, the client is authenticated.

NOTE: The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.

ip ssh authentication-retries

This command configures the number of times the SSH server attempts to reauthenticate a user. Use the **no** form to restore the default setting.

SYNTAX

ip ssh authentication-retries *count*

no ip ssh authentication-retries

count – The number of authentication attempts permitted after which the interface is reset. (Range: 1-5)

DEFAULT SETTING

3

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#ip ssh authentication-retires 2
Console(config)#
```

RELATED COMMANDS

show ip ssh (588)

ip ssh server

This command enables the Secure Shell (SSH) server on this switch. Use the **no** form to disable this service.

SYNTAX

[**no**] **ip ssh server**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.
- The SSH server uses DSA or RSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.
- You must generate DSA and RSA host keys before enabling the SSH server.

EXAMPLE

```
Console#ip ssh crypto host-key generate dsa
Console#configure
Console(config)#ip ssh server
Console(config)#
```

RELATED COMMANDS

ip ssh crypto host-key generate (586)
show ssh (589)

ip ssh server-key size

This command sets the SSH server key size. Use the **no** form to restore the default setting.

SYNTAX

ip ssh server-key size *key-size*

no ip ssh server-key size

key-size – The size of server key. (Range: 512-896 bits)

DEFAULT SETTING
768 bits

COMMAND MODE
Global Configuration

COMMAND USAGE
The server key is a private key that is never shared outside the switch. The host key is shared with the SSH client, and is fixed at 1024 bits.

EXAMPLE

```
Console(config)#ip ssh server-key size 512
Console(config)#
```

ip ssh timeout

This command configures the timeout for the SSH server. Use the **no** form to restore the default setting.

SYNTAX

ip ssh timeout *seconds*

no ip ssh timeout

seconds – The timeout for client response during SSH negotiation. (Range: 1-120)

DEFAULT SETTING
10 seconds

COMMAND MODE
Global Configuration

COMMAND USAGE
The **timeout** specifies the interval the switch will wait for a response from the client during the SSH negotiation phase. Once an SSH session has been established, the timeout for user input is controlled by the exec-timeout command for vty sessions.

EXAMPLE

```
Console(config)#ip ssh timeout 60
Console(config)#
```

RELATED COMMANDS
exec-timeout (483)
show ip ssh (588)

delete public-key

This command deletes the specified user's public key.

SYNTAX

delete public-key *username* [**dsa** | **rsa**]

username – Name of an SSH user. (Range: 1-8 characters)

dsa – DSA public key type.

rsa – RSA public key type.

DEFAULT SETTING

Deletes both the DSA and RSA key.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#delete public-key admin dsa
Console#
```

ip ssh crypto host-key generate

This command generates the host key pair (i.e., public and private).

SYNTAX

ip ssh crypto host-key generate [**dsa** | **rsa**]

dsa – DSA (Version 2) key type.

rsa – RSA (Version 1) key type.

DEFAULT SETTING

Generates both the DSA and RSA key pairs.

COMMAND MODE

Privileged Exec

COMMAND USAGE

- The switch uses only RSA Version 1 for SSHv1.5 clients and DSA Version 2 for SSHv2 clients.
- This command stores the host key pair in memory (i.e., RAM). Use the ip ssh save host-key command to save the host key pair to flash memory.
- Some SSH client programs automatically add the public key to the known hosts file as part of the configuration process. Otherwise, you must manually create a known hosts file and place the host public key in it.
- The SSH server uses this host key to negotiate a session key and encryption method with the client trying to connect to it.

EXAMPLE

```
Console#ip ssh crypto host-key generate dsa
Console#
```

RELATED COMMANDS

ip ssh crypto zeroize (587)
ip ssh save host-key (587)

ip ssh crypto zeroize

This command clears the host key from memory (i.e. RAM).

SYNTAX

ip ssh crypto zeroize [**dsa** | **rsa**]

dsa – DSA key type.

rsa – RSA key type.

DEFAULT SETTING

Clears both the DSA and RSA key.

COMMAND MODE

Privileged Exec

COMMAND USAGE

- This command clears the host key from volatile memory (RAM). Use the **no** ip ssh save host-key command to clear the host key from flash memory.
- The SSH server must be disabled before you can execute this command.

EXAMPLE

```
Console#ip ssh crypto zeroize dsa
Console#
```

RELATED COMMANDS

ip ssh crypto host-key generate (586)
ip ssh save host-key (587)
no ip ssh server (584)

ip ssh save host-key

This command saves the host key from RAM to flash memory.

SYNTAX

ip ssh save host-key

DEFAULT SETTING
Saves both the DSA and RSA key.

COMMAND MODE
Privileged Exec

EXAMPLE
```
Console#ip ssh save host-key dsa
Console#
```

RELATED COMMANDS
ip ssh crypto host-key generate (586)

show ip ssh
This command displays the connection settings used when authenticating client access to the SSH server.

COMMAND MODE
Privileged Exec

EXAMPLE
```
Console#show ip ssh
SSH Enabled - Version 2.0
Negotiation Timeout : 120 seconds; Authentication Retries : 3
Server Key Size     : 768 bits
Console#
```

show public-key
This command shows the public key for the specified user or for the host.

SYNTAX
show public-key [**user** [*username*]| **host**]

username – Name of an SSH user. (Range: 1-8 characters)

DEFAULT SETTING
Shows all public keys.

COMMAND MODE
Privileged Exec

COMMAND USAGE
- If no parameters are entered, all keys are displayed. If the user keyword is entered, but no user name is specified, then the public keys for all users are displayed.
- When an RSA key is displayed, the first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 35), and the last string is the encoded modulus. When a DSA key

is displayed, the first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS), and the last string is the encoded modulus.

EXAMPLE

```
Console#show public-key host
Host:
RSA:
1024 65537 13236940658254764031382795526536375927835525327972629521130241
  07194210616557594245909392360969540503627752575562510038661309893938345231 0
  33280214988866192159556859887989191950588394018138744046890877916030583776 8
  18549000283134162500834871844952208742921225569166565529632816351696404083 1
  5547660664151657116381
DSA:
ssh-dss AAAB3NzaC1kc3MAAACBAPWKZTPbsRIB8ydEXcxM3dyV/yrDbKStIlnzD/Dg0h2Hxc
  YV44sXZ2JXhamLK6P8bvuiyacWbUW/a4PAtp1KMSdqsKeh3hKoA3vRRSy1N2XFfAKxl5fwFfv
  JlPdOkFgzLGMinvSNYQwiQXbKTBH0Z4mUZpE85PWxDZMaCNBPjBrRAAAAFQChb4vsdfQGNIjwbv
  wrNLaQ77isiwAAAIEAsy5YWDC99ebYHNRj5kh47wY4i8cZvH+/p9cnrfwFTMU01VFDly3IR
  2G395NLy5Qd7ZDxfA9mCOfT/yyEfbobMJZi8oGCstSNOxrZZVnMqWrTYfdrKX7YKBw/Kjw6Bm
  iFq7O+jAhf1Dg45loAc27s6TLdtny1wRq/ow2eTCD5nekAAACBAJ8rMccXTxHLFAczWS7EjOy
  DbsloBfPuSAb4oAsyjKXKVYNLQkTLZfcFRu41bS2KV5LAwecsigF/+DjKGWtPNIQqabKgYCw2
  o/dVzX4Gg+yqdTlYmGA7fHGm8ARGeiG4ssFKy4Z6DmYPXFum1Yg0fhLwuHpOSKdxT3kk475S7
  w0W
Console#
```

show ssh

This command displays the current SSH server connections.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ssh
Connection Version State                Username Encryption
  0          2.0   Session-Started      admin    ctos aes128-cbc-hmac-md5
                                                 stoc aes128-cbc-hmac-md5
Console#
```

Table 71: show ssh - display description

Field	Description
Session	The session number. (Range: 0-3)
Version	The Secure Shell version number.
State	The authentication negotiation state. (Values: Negotiation-Started, Authentication-Started, Session-Started)
Username	The user name of the client.

802.1X PORT AUTHENTICATION

The switch supports IEEE 802.1X (dot1x) port-based access control that prevents unauthorized access to the network by requiring users to first submit credentials for authentication. Client authentication is controlled centrally by a RADIUS server using EAP (Extensible Authentication Protocol).

Table 72: 802.1X Port Authentication Commands

Command	Function	Mode
General Commands		
dot1x default	Resets all dot1x parameters to their default values	GC
dot1x eapol-pass-through	Passes EAPOL frames to all ports in STP forwarding state when dot1x is globally disabled	GC
dot1x system-auth-control	Enables dot1x globally on the switch.	GC
Authenticator Commands		
dot1x intrusion-action	Sets the port response to intrusion when authentication fails	IC
dot1x max-req	Sets the maximum number of times that the switch retransmits an EAP request/identity packet to the client before it times out the authentication session	IC
dot1x operation-mode	Allows single or multiple hosts on an dot1x port	IC
dot1x port-control	Sets dot1x mode for a port interface	IC
dot1x re-authentication	Enables re-authentication for all ports	IC
dot1x timeout quiet-period	Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client	IC
dot1x timeout re-authperiod	Sets the time period after which a connected client must be re-authenticated	IC
dot1x timeout supp-timeout	Sets the interval for a supplicant to respond	IC
dot1x timeout tx-period	Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet	IC
dot1x re-authenticate	Forces re-authentication on specific ports	PE
Supplicant Commands		
dot1x identity profile	Configures dot1x supplicant user name and password	GC
dot1x max-start	Sets the maximum number of times that a port supplicant will send an EAP start frame to the client	IC
dot1x pae supplicant	Enables dot1x supplicant mode on an interface	IC
dot1x timeout auth-period	Sets the time that a supplicant port waits for a response from the authenticator	IC
dot1x timeout held-period	Sets the time a port waits after the maximum start count has been exceeded before attempting to find another authenticator	IC

Table 72: 802.1X Port Authentication Commands (Continued)

Command	Function	Mode
dot1x timeout start-period	Sets the time that a supplicant port waits before resending an EAPOL start frame to the authenticator	IC
Display Information Commands		
show dot1x	Shows all dot1x related information	PE

dot1x default

This command sets all configurable dot1x global and port settings to their default values.

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#dot1x default
Console(config)#
```

dot1x eapol-pass-through

This command passes EAPOL frames through to all ports in STP forwarding state when dot1x is globally disabled. Use the **no** form to restore the default.

SYNTAX

[**no**] **dot1x eapol-pass-through**

DEFAULT SETTING

Discards all EAPOL frames when dot1x is globally disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- When this device is functioning as intermediate node in the network and does not need to perform dot1x authentication, the **dot1x eapol pass-through** command can be used to forward EAPOL frames from other switches on to the authentication servers, thereby allowing the authentication process to still be carried out by switches located on the edge of the network.

- When this device is functioning as an edge switch but does not require any attached clients to be authenticated, the **no dot1x eapol-pass-through** command can be used to discard unnecessary EAPOL traffic.

EXAMPLE

This example instructs the switch to pass all EAPOL frame through to any ports in STP forwarding state.

```
Console(config)#dot1x eapol-pass-through
Console(config)#
```

dot1x system-auth-control

This command enables IEEE 802.1X port authentication globally on the switch. Use the **no** form to restore the default.

SYNTAX

[**no**] **dot1x system-auth-control**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#dot1x system-auth-control
Console(config)#
```

dot1x intrusion-action

This command sets the port's response to a failed authentication, either to block all traffic, or to assign all traffic for the port to a guest VLAN. Use the **no** form to reset the default.

SYNTAX

dot1x intrusion-action {**block-traffic** | **guest-vlan**}

no dot1x intrusion-action

block-traffic - Blocks traffic on this port.

guest-vlan - Assigns the user to the Guest VLAN.

DEFAULT

block-traffic

COMMAND MODE

Interface Configuration

COMMAND USAGE

For guest VLAN assignment to be successful, the VLAN must be configured and set as active (see the vlan database command) and assigned as the guest VLAN for the port (see the network-access guest-vlan command).

EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x intrusion-action guest-vlan
Console(config-if)#
```

dot1x max-req

This command sets the maximum number of times the switch port will retransmit an EAP request/identity packet to the client before it times out the authentication session. Use the **no** form to restore the default.

SYNTAX

dot1x max-req *count*

no dot1x max-req

count – The maximum number of requests (Range: 1-10)

DEFAULT

2

COMMAND MODE

Interface Configuration

EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-req 2
Console(config-if)#
```

dot1x operation-mode

This command allows hosts (clients) to connect to an 802.1X-authorized port. Use the **no** form with no keywords to restore the default to single host. Use the **no** form with the **multi-host max-count** keywords to restore the default maximum count.

SYNTAX

dot1x operation-mode {**single-host** | **multi-host** [**max-count** *count*] | **mac-based-auth**}

no dot1x operation-mode [**multi-host max-count**]

single-host – Allows only a single host to connect to this port.

multi-host – Allows multiple host to connect to this port.

max-count – Keyword for the maximum number of hosts.

count – The maximum number of hosts that can connect to a port. (Range: 1-1024; Default: 5)

mac-based – Allows multiple hosts to connect to this port, with each host needing to be authenticated.

DEFAULT
Single-host

COMMAND MODE
Interface Configuration

COMMAND USAGE
- The "max-count" parameter specified by this command is only effective if the dot1x mode is set to "auto" by the dot1x port-control command.
- In "multi-host" mode, only one host connected to a port needs to pass authentication for all other hosts to be granted network access. Similarly, a port can become unauthorized for all hosts if one attached host fails re-authentication or sends an EAPOL logoff message.
- In "mac-based-auth" mode, each host connected to a port needs to pass authentication. The number of hosts allowed access to a port operating in this mode is limited only by the available space in the secure address table (i.e., up to 1024 addresses).

EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x operation-mode multi-host max-count 10
Console(config-if)#
```

dot1x port-control

This command sets the dot1x mode on a port interface. Use the **no** form to restore the default.

SYNTAX

dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**}

no dot1x port-control

auto – Requires a dot1x-aware connected client to be authorized by the RADIUS server. Clients that are not dot1x-aware will be denied access.

force-authorized – Configures the port to grant access to all clients, either dot1x-aware or otherwise.

force-unauthorized – Configures the port to deny access to all clients, either dot1x-aware or otherwise.

DEFAULT
force-authorized

COMMAND MODE
Interface Configuration

EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x port-control auto
Console(config-if)#
```

dot1x re-authentication

This command enables periodic re-authentication for a specified port. Use the **no** form to disable re-authentication.

SYNTAX

[**no**] **dot1x re-authentication**

COMMAND MODE

Interface Configuration

COMMAND USAGE

- The re-authentication process verifies the connected client's user ID and password on the RADIUS server. During re-authentication, the client remains connected the network and the process is handled transparently by the dot1x client software. Only if re-authentication fails is the port blocked.
- The connected client is re-authenticated after the interval specified by the dot1x timeout re-authperiod command. The default is 3600 seconds.

EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x re-authentication
Console(config-if)#
```

RELATED COMMANDS

dot1x timeout re-authperiod (596)

dot1x timeout quiet-period

This command sets the time that a switch port waits after the maximum request count (see page 593) has been exceeded before attempting to acquire a new client. Use the **no** form to reset the default.

SYNTAX

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

seconds - The number of seconds. (Range: 1-65535)

DEFAULT

60 seconds

COMMAND MODE
Interface Configuration

EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout quiet-period 350
Console(config-if)#
```

dot1x timeout re-authperiod

This command sets the time period after which a connected client must be re-authenticated. Use the **no** form of this command to reset the default.

SYNTAX

dot1x timeout re-authperiod *seconds*

no dot1x timeout re-authperiod

seconds - The number of seconds. (Range: 1-65535)

DEFAULT
3600 seconds

COMMAND MODE
Interface Configuration

EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout re-authperiod 300
Console(config-if)#
```

dot1x timeout supp-timeout

This command sets the time that an interface on the switch waits for a response to an EAP request from a client before re-transmitting an EAP packet. Use the **no** form to reset to the default value.

SYNTAX

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

seconds - The number of seconds. (Range: 1-65535)

DEFAULT
30 seconds

COMMAND MODE
Interface Configuration

COMMAND USAGE

This command sets the timeout for EAP-request frames other than EAP-request/identity frames. If dot1x authentication is enabled on a port, the switch will initiate authentication when the port link state comes up. It will send an EAP-request/identity frame to the client to request its identity, followed by one or more requests for authentication information. It may also send other EAP-request frames to the client during an active connection as required for reauthentication.

EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout supp-timeout 300
Console(config-if)#
```

dot1x timeout tx-period

This command sets the time that an interface on the switch waits during an authentication session before re-transmitting an EAP packet. Use the **no** form to reset to the default value.

SYNTAX

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

seconds - The number of seconds. (Range: 1-65535)

DEFAULT

30 seconds

COMMAND MODE

Interface Configuration

EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout tx-period 300
Console(config-if)#
```

dot1x re-authenticate

This command forces re-authentication on all ports or a specific interface.

SYNTAX

dot1x re-authenticate [**interface** *interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10)

COMMAND MODE
Privileged Exec

COMMAND USAGE
The re-authentication process verifies the connected client's user ID and password on the RADIUS server. During re-authentication, the client remains connected the network and the process is handled transparently by the dot1x client software. Only if re-authentication fails is the port blocked.

EXAMPLE

```
Console#dot1x re-authenticate
Console#
```

dot1x identity profile

This command sets the dot1x supplicant user name and password. Use the **no** form to delete the identity settings.

SYNTAX

dot1x identity profile {**username** *username* | **password** *password*}

no dot1x identity profile {**username** | **password**}

username - Specifies the supplicant user name. (Range: 1-8 characters)

password - Specifies the supplicant password. (Range: 1-8 characters)

DEFAULT
No user name or password

COMMAND MODE
Global Configuration

COMMAND USAGE
The global supplicant user name and password are used to identify this switch as a supplicant when responding to an MD5 challenge from the authenticator. These parameters must be set when this switch passes client authentication requests to another authenticator on the network (see the dot1x pae supplicant command on page 599).

EXAMPLE

```
Console(config)#dot1x identity profile username steve
Console(config)#dot1x identity profile password excess
Console(config)#
```

dot1x max-start

This command sets the maximum number of times that a port supplicant will send an EAP start frame to the client before assuming that the client is 802.1X unaware. Use the **no** form to restore the default value.

SYNTAX

dot1x max-start *count*

no dot1x max-start

count - Specifies the maximum number of EAP start frames. (Range: 1-65535)

DEFAULT

3

COMMAND MODE

Interface Configuration

EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-start 10
Console(config-if)#
```

dot1x pae supplicant

This command enables dot1x supplicant mode on a port. Use the **no** form to disable dot1x supplicant mode on a port.

SYNTAX

[**no**] **dot1x pae supplicant**

DEFAULT

Disabled

COMMAND MODE

Interface Configuration

COMMAND USAGE

- When devices attached to a port must submit requests to another authenticator on the network, configure the identity profile parameters (see dot1x identity profile command on page 598) which identify this switch as a supplicant, and enable dot1x supplicant mode for those ports which must authenticate clients through a remote authenticator using this command. In this mode the port will not respond to dot1x messages meant for an authenticator.

- This switch can be configured to serve as the authenticator on selected ports by setting the control mode to "auto" (see the dot1x port-control command on page 594), and as a supplicant on other ports by the setting the control mode to "force-authorized" and enabling dot1x supplicant mode with this command.

- A port cannot be configured as a dot1x supplicant if it is a member of a trunk or LACP is enabled on the port.

EXAMPLE

```
Console(config)#interface ethernet 1/2
Console(config-if)#dot1x pae supplicant
Console(config-if)#
```

dot1x timeout auth-period

This command sets the time that a supplicant port waits for a response from the authenticator. Use the **no** form to res store the default setting.

SYNTAX

dot1x timeout auth-period *seconds*

no dot1x timeout auth-period

seconds - The number of seconds. (Range: 1-65535)

DEFAULT

30 seconds

COMMAND MODE

Interface Configuration

COMMAND USAGE

This command sets the time that the supplicant waits for a response from the authenticator for packets other than EAPOL-Start.

EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout auth-period 60
Console(config-if)#
```

dot1x timeout held-period

This command sets the time that a supplicant port waits before resending its credentials to find a new an authenticator. Use the **no** form to reset the default.

SYNTAX

dot1x timeout held-period *seconds*

no dot1x timeout held-period

seconds - The number of seconds. (Range: 1-65535)

DEFAULT

60 seconds

COMMAND MODE
Interface Configuration

EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout held-period 120
Console(config-if)#
```

dot1x timeout start-period

This command sets the time that a supplicant port waits before resending an EAPOL start frame to the authenticator. Use the **no** form to restore the default setting.

SYNTAX

dot1x timeout start-period *seconds*

no dot1x timeout start-period

seconds - The number of seconds. (Range: 1-65535)

DEFAULT
30 seconds

COMMAND MODE
Interface Configuration

EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout start-period 60
Console(config-if)#
```

show dot1x

This command shows general port authentication related settings on the switch or a specific interface.

SYNTAX

show dot1x [**statistics**] [**interface** *interface*]

statistics - Displays dot1x status for each port.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-10)

COMMAND MODE
Privileged Exec

COMMAND USAGE

This command displays the following information:

- *Global 802.1X Parameters* – Shows whether or not 802.1X port authentication is globally enabled on the switch (page 592).
- *Authenticator Parameters* – Shows whether or not EAPOL pass-through is enabled (page 591).
- *Supplicant Parameters* – Shows the supplicant user name used when the switch responds to an MD5 challenge from an authenticator (page 598).
- *802.1X Port Summary* – Displays the port access control parameters for each interface that has enabled 802.1X, including the following items:
  - Type – Administrative state for port access control (Enabled, Authenticator, or Supplicant).
  - Operation Mode–Allows single or multiple hosts (page 593).
  - Mode– Dot1x port control mode (page 594).
  - Authorized– Authorization status (yes or n/a - not authorized).
- *802.1X Port Details* – Displays the port access control parameters for each interface, including the following items:
  - Reauthentication – Periodic re-authentication (page 595).
  - Reauth Period – Time after which a connected client must be re-authenticated (page 596).
  - Quiet Period – Time a port waits after Max Request Count is exceeded before attempting to acquire a new client (page 595).
  - TX Period – Time a port waits during authentication session before re-transmitting EAP packet (page 597).
  - Supplicant Timeout – Supplicant timeout.
  - Server Timeout – Server timeout.
  - Reauth Max Retries – Maximum number of reauthentication attempts.
  - Max Request – Maximum number of times a port will retransmit an EAP request/identity packet to the client before it times out the authentication session (page 593).
  - Operation Mode– Shows if single or multiple hosts (clients) can connect to an 802.1X-authorized port.
  - Port Control–Shows the dot1x mode on a port as auto, force-authorized, or force-unauthorized (page 594).
  - Intrusion Action– Sets the port response to intrusion when authentication fails (page 592).
  - Supplicant– MAC address of authorized client.
- *Authenticator State Machine*
  - State – Current state (including initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized).
  - Reauth Count– Number of times connecting state is re-entered.

- Current Identifier– The integer (0-255) used by the Authenticator to identify the current authentication session.

- *Backend State Machine*

  - State – Current state (including request, response, success, fail, timeout, idle, initialize).
  - Request Count– Number of EAP Request packets sent to the Supplicant without receiving a response.
  - Identifier (Server)– Identifier carried in the most recent EAP Success, Failure or Request packet received from the Authentication Server.

- *Reauthentication State Machine*

  State – Current state (including initialize, reauthenticate).

EXAMPLE

```
Console#show dot1x
Global 802.1X Parameters
  System-auth-control: Enabled

Authenticator Parameters:
 EAPOL Pass Through        : Disabled

Supplicant Parameters:
 Identity Profile Username : steve

802.1X Port Summary

Port Name  Status        Operation Mode   Mode                Authorized
1/1        Disabled      Single-Host      ForceAuthorized     N/A
1/2        Disabled      Single-Host      ForceAuthorized     N/A
.
.
.
1/27       Disabled      Single-Host      ForceAuthorized     Yes
1/28       Enabled       Single-Host      Auto                Yes

802.1X Port Details

802.1X Authenticator is enabled on port 1/1
802.1X Supplicant is disabled on port 1/1
.
.
.
802.1X Authenticator is enabled on port 10
Reauthentication     : Enabled
Reauth Period        : 3600
Quiet Period         : 60
TX Period            : 30
Supplicant Timeout   : 30
Server Timeout       : 10
Reauth Max Retries   : 2
Max Request          : 2
Operation Mode       : Multi-host
Port Control         : Auto
Intrusion action     : Block traffic

Supplicant           : 00-e0-29-94-34-65
```

```
Authenticator State Machine
State                : Authenticated
Reauth Count         : 0
Current Identifier   : 3

Backend State Machine
State                : Idle
Request Count        : 0
Identifier(Server)   : 2

Reauthentication State Machine
State                : Initialize

Console#
```

MANAGEMENT IP FILTER

This section describes commands used to configure IP management access to the switch.

Table 73: Management IP Filter Commands

Command	Function	Mode
management	Configures IP addresses that are allowed management access	GC
show management	Displays the switch to be monitored or configured from a browser	PE

management

This command specifies the client IP addresses that are allowed management access to the switch through various protocols. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **management** {**all-client** | **http-client** | **snmp-client** | **telnet-client**} *start-address* [*end-address*]

all-client - Adds IP address(es) to all groups.

http-client - Adds IP address(es) to the web group.

snmp-client - Adds IP address(es) to the SNMP group.

telnet-client - Adds IP address(es) to the Telnet group.

start-address - A single IP address, or the starting address of a range.

end-address - The end address of a range.

DEFAULT SETTING

All addresses

COMMAND MODE

Global Configuration

COMMAND USAGE

- If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- IP address can be configured for SNMP, web, and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.
- When entering addresses for the same group (i.e., SNMP, web, or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.
- You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.
- You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

EXAMPLE

This example restricts management access to the indicated addresses.

```
Console(config)#management all-client 192.168.1.19
Console(config)#management all-client 192.168.1.25 192.168.1.30
Console#
```

show management

This command displays the client IP addresses that are allowed management access to the switch through various protocols.

SYNTAX

show management {**all-client** | **http-client** | **snmp-client** | **telnet-client**}

all-client - Displays IP addresses for all groups.

http-client - Displays IP addresses for the web group.

snmp-client - Displays IP addresses for the SNMP group.

telnet-client - Displays IP addresses for the Telnet group.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show management all-client
Management Ip Filter
 HTTP-Client:
   Start IP address      End IP address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

 SNMP-Client:
   Start IP address      End IP address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

 TELNET-Client:
   Start IP address      End IP address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

Console#
```

PPPOE INTERMEDIATE AGENT

This section describes commands used to configure the PPoE Intermediate Agent (PPPoE IA) relay parameters required for passing authentication messages between a client and broadband remote access servers.

Table 74: PPPoE Intermediate Agent Commands

Command	Function	Mode
pppoe intermediate-agent	Enables the PPPoE IA globally on the switch	GC
pppoe intermediate-agent format-type	Sets the access node identifier and generic error message for the switch	GC
pppoe intermediate-agent port-enable	Enables the PPPoE IA on an interface	IC
pppoe intermediate-agent port-format-type	Sets the circuit-id or remote-id for an interface	IC
pppoe intermediate-agent trust	Sets the trust mode for an interface	IC
pppoe intermediate-agent vendor-tag strip	Enables the stripping of vendor tags from PPPoE Discovery packets sent from a PPPoE server	IC
clear pppoe intermediate-agent statistics	Clears PPPoE IA statistics	PE
show pppoe intermediate-agent info	Displays PPPoE IA configuration settings	PE
show pppoe intermediate-agent statistics	Displays PPPoE IA statistics	PE

pppoe intermediate-agent

This command enables the PPPoE Intermediate Agent globally on the switch. Use the **no** form to disable this feature.

SYNTAX

[**no**] **pppoe intermediate-agent**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- The switch inserts a tag identifying itself as a PPPoE Intermediate Agent residing between the attached client requesting network access and the ports connected to broadband remote access servers (BRAS). The switch extracts access-loop information from the client's PPPoE Active Discovery Request, and forwards this information to all trusted ports designated by the pppoe intermediate-agent trust command. The BRAS detects the presence of the subscriber's circuit-Id tag inserted by the switch during the PPPoE discovery phase, and sends this tag as a NAS-port-Id attribute in PPP authentication and AAA accounting requests to a RADIUS server.

- PPPoE IA must be enabled globally by this command before this feature can be enabled on an interface using the pppoe intermediate-agent port-enable command.

EXAMPLE

```
Console(config)#pppoe intermediate-agent
Console(config)#
```

pppoe intermediate-agent format-type

This command sets the access node identifier and generic error message for the switch. Use the **no** form to restore the default settings.

SYNTAX

pppoe intermediate-agent format-type {**access-node-identifier** *id-string* | **generic-error-message** *error-message*}

no pppoe intermediate-agent format-type {**access-node-identifier** | **generic-error-message**}

id-string - String identifying this switch as an PPPoE IA to the PPPoE server. (Range: 1-48 ASCII characters)

error-message - An error message notifying the sender that the PPPoE Discovery packet was too large.

DEFAULT SETTING

- Access Node Identifier: IP address of the management interface
- Generic Error Message: PPPoE Discover packet too large to process. Try reducing the number of tags added.

COMMAND MODE

Global Configuration

COMMAND USAGE

- The switch uses the access-node-identifier to generate the circuit-id for PPPoE discovery stage packets sent to the BRAS, but does not modify the source or destination MAC address of these PPPoE discovery packets.
- These messages are forwarded to all trusted ports designated by the pppoe intermediate-agent trust command.

EXAMPLE

```
Console(config)#pppoe intermediate-agent format-type access-node-identifier
  billibong
Console(config)#
```

pppoe intermediate-agent port-enable

This command enables the PPPoE IA on an interface. Use the **no** form to disable this feature.

SYNTAX

[**no**] **pppoe intermediate-agent port-enable**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

PPPoE IA must also be enabled globally on the switch for this command to tack effect.

EXAMPLE

```
Console(config)#int ethernet 1/5
Console(config-if)#pppoe intermediate-agent port-enable
Console(config-if)#
```

pppoe intermediate-agent port-format-type

This command sets the circuit-id or remote-id for an interface. Use the **no** form to restore the default settings.

SYNTAX

pppoe intermediate-agent port-format-type {**circuit-id** | **remote-id**} *id-string*

circuit-id - String identifying the circuit identifier (or interface) on this switch to which the user is connected. (Range: 1-10 ASCII characters)

remote-id - String identifying the remote identifier (or interface) on this switch to which the user is connected. (Range: 1-63 ASCII characters)

DEFAULT SETTING

circuit-id: unit/port:vlan-id or 0/trunk-id:vlan-id
remote-id: port MAC address

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- The PPPoE server extracts the Line-Id tag from PPPoE discovery stage messages, and uses the Circuit-Id field of that tag as a NAS-Port-Id attribute in AAA access and accounting requests.
- The switch intercepts PPPoE discovery frames from the client and inserts a unique line identifier using the PPPoE Vendor-Specific tag (0x0105) to PPPoE Active Discovery Initiation (PADI) and Request (PADR) packets. The switch then forwards these packets to the PPPoE server. The tag contains the Line-Id of the customer line over which the discovery packet was received, entering the switch (or access node) where the intermediate agent resides.
- Outgoing PAD Offer (PADO) and Session-confirmation (PADS) packets sent from the PPPoE Server include the Circuit-Id tag inserted by the switch, and should be stripped out of PADO and PADS packets which are to be passed directly to end-node clients using the pppoe intermediate-agent vendor-tag strip command.

EXAMPLE

```
Console(config)#int ethernet 1/5
Console(config-if)#pppoe intermediate-agent port-enable
Console(config-if)#
```

pppoe intermediate-agent trust

This command sets an interface to trusted mode to indicate that it is connected to a PPPoE server. Use the **no** form to set an interface to untrusted mode.

SYNTAX

[**no**] **pppoe intermediate-agent trust**

DEFAULT SETTING

Untrusted

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- Set any interfaces connecting the switch to a PPPoE Server as trusted. Interfaces that connect the switch to users (PPPoE clients) should be set as untrusted.
- At least one trusted interface must be configured on the switch for the PPPoE IA to function.

EXAMPLE

```
Console(config)#int ethernet 1/5
Console(config-if)#pppoe intermediate-agent trust
Console(config-if)#
```

pppoe intermediate-agent vendor-tag strip

This command enables the stripping of vendor tags from PPPoE Discovery packets sent from a PPPoE server. Use the **no** form to disable this feature.

SYNTAX

[**no**] **pppoe intermediate-agent vendor-tag strip**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This command only applies to trusted interfaces. It is used to strip off vendor-specific tags (which carry subscriber and line identification information) in PPPoE Discovery packets received from an upstream PPPoE server before forwarding them to a user.

EXAMPLE

```
Console(config)#int ethernet 1/5
Console(config-if)#pppoe intermediate-agent vendor-tag strip
Console(config-if)#
```

clear pppoe intermediate-agent statistics

This command clears statistical counters for the PPPoE Intermediate Agent.

SYNTAX

clear pppoe intermediate-agent statistics interface [*interface*]

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#clear pppoe intermediate-agent statistics
Console#
```

show pppoe intermediate-agent info

This command displays configuration settings for the PPPoE Intermediate Agent.

SYNTAX

show pppoe intermediate-agent info [**interface** [*interface*]]

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show pppoe intermediate-agent info
PPPoE Intermediate Agent Global Status          : Enabled
PPPoE Intermediate Agent Access Node Identifier :
 192.168.0.2
```

```
PPPoE Intermediate Agent Generic Error Message  :
 PPPoE Discover packet too large to process. Try reducing the number of tags
  added.
Consoleshowpppoe intermediate-agent info interface ethernet 1/1
Interface PPPoE IA Trusted Vendor-Tag Strip Circuit-ID   Remote-ID
--------- -------- ------- ---------------- ------------ -----------------
Eth 1/1   Yes      Yes     Yes              1/1:vid      00-12-CF-61-24-30
Console#
```

show pppoe intermediate-agent statistics

This command displays statistics for the PPPoE Intermediate Agent.

SYNTAX

show pppoe intermediate-agent statistics interface [*interface*]

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show pppoe intermediate-agent statistics interface ethernet 1/1
Eth 1/1 statistics
------------------------------------------------------------------------------
 Received :        All       PADI       PADO       PADR       PADS       PADT
            ---------- ---------- ---------- ---------- ---------- ----------
                     3          0          0          0          0          3

 Dropped  : Response from untrusted  Request towards untrusted  Malformed
            ------------------------  --------------------------  ---------
                                   0                           0          0
Console#
```

Table 75: show pppoe intermediate-agent statistics - display description

Field	Description
PADI	PPPoE Active Discovery Initiation
PADO	PPPoE Active Discovery Offer
PADR	PPPoE Active Discovery Request
PADS	PPPoE Active Discovery Session-Confirmation
PADT	PPPoE Active Discovery Terminate

25 GENERAL SECURITY MEASURES

This switch supports many methods of segregating traffic for clients attached to each of the data ports, and for ensuring that only authorized clients gain access to the network. Private VLANs and port-based authentication using IEEE 802.1X are commonly used for these purposes. In addition to these method, several other options of providing client security are described in this chapter. These include port-based authentication, which can be configured to allow network client access by specifying a fixed set of MAC addresses. The addresses assigned to DHCP clients can also be carefully controlled with IP Source Guard and DHCP Snooping commands.

Table 76: General Security Commands

Command Group	Function
Port Security*	Configures secure addresses for a port
802.1X Port Authentication*	Configures host authentication on specific ports using 802.1X
Network Access*	Configures MAC authentication and dynamic VLAN assignment
Web Authentication*	Configures Web authentication
Access Control Lists*	Provides filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or non-IP frames (based on MAC address or Ethernet type)
DHCP Snooping*	Filters untrusted DHCP messages on unsecure ports by building and maintaining a DHCP snooping binding table
IP Source Guard*	Filters IP traffic on insecure ports for which the source address cannot be identified via DHCP snooping nor static source bindings
ARP Inspection	Validates the MAC-to-IP address bindings in ARP packets

* The priority of execution for these filtering commands is Port Security, Port Authentication, Network Access, Web Authentication, Access Control Lists, DHCP Snooping, and then IP Source Guard.

PORT SECURITY

These commands can be used to enable port security on a port.

When using port security, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table for this port will be authorized to access the network. The port will drop any incoming frames with a source MAC address that is unknown or has been previously learned from another port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

Table 77: Management IP Filter Commands

Command	Function	Mode
mac-address-table static	Maps a static address to a port in a VLAN	GC
port security	Configures a secure port	IC
show mac-address-table	Displays entries in the bridge-forwarding database	PE

port security

This command enables or configures port security. Use the **no** form without any keywords to disable port security. Use the **no** form with the appropriate keyword to restore the default settings for a response to security violation or for the maximum number of allowed addresses.

SYNTAX

port security [**action** {**shutdown** | **trap** | **trap-and-shutdown**} | **max-mac-count** *address-count*]

no port security [**action** | **max-mac-count**]

action - Response to take when port security is violated.

shutdown - Disable port only.

trap - Issue SNMP trap message only.

trap-and-shutdown - Issue SNMP trap message and disable port.

max-mac-count

address-count - The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 1024, where 0 means disabled)

DEFAULT SETTING

Status: Disabled
Action: None
Maximum Addresses: 0

COMMAND MODE
Interface Configuration (Ethernet)

COMMAND USAGE
- When port security is enabled with this command, the switch first clears all dynamically learned entries from the address table. It then starts learning new MAC addresses on the specified port, and stops learning addresses when it reaches a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted.

- First use the **port security max-mac-count** command to set the number of addresses, and then use the **port security** command to enable security on the port. (The specified maximum address count is effective when port security is enabled or disabled.)

- Use the **no port security max-mac-count** command to disable port security and reset the maximum number of addresses to the default.

- You can also manually add secure addresses with the mac-address-table static command.

- A secure port has the following restrictions:

  - Cannot be connected to a network interconnection device.
  - Cannot be a trunk port.

- If a port is disabled due to a security violation, it must be manually re-enabled using the no shutdown command.

EXAMPLE
The following example enables port security for port 5, and sets the response to a security violation to issue a trap message:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap
```

RELATED COMMANDS
show interfaces status (694)
shutdown (688)
mac-address-table static (740)

NETWORK ACCESS (MAC ADDRESS AUTHENTICATION)

Network Access authentication controls access to the network by authenticating the MAC address of each host that attempts to connect to a switch port. Traffic received from a specific MAC address is forwarded by the switch only if the source MAC address is successfully authenticated by a central RADIUS server. While authentication for a MAC address is in progress, all traffic is blocked until authentication is completed. Once successfully authenticated, the RADIUS server may optionally assign VLAN and QoS settings for the switch port.

Table 78: Network Access Commands

Command	Function	Mode
network-access aging	Enables MAC address aging	GC
network-access mac-filter	Adds a MAC address to a filter table	GC
mac-authentication reauth-time	Sets the time period after which a connected MAC address must be re-authenticated	GC
network-access dynamic-qos	Enables the dynamic quality of service feature	IC
network-access dynamic-vlan	Enables dynamic VLAN assignment from a RADIUS server	IC
network-access guest-vlan	Specifies the guest VLAN	IC
network-access link-detection	Enables the link detection feature	IC
network-access link-detection link-down	Configures the link detection feature to detect and act upon link-down events	IC
network-access link-detection link-up	Configures the link detection feature to detect and act upon link-up events	IC
network-access link-detection link-up-down	Configures the link detection feature to detect and act upon both link-up and link-down events	IC
network-access max-mac-count	Sets the maximum number of MAC addresses that can be authenticated on a port via all forms of authentication	IC
network-access mode mac-authentication	Enables MAC authentication on an interface	IC
network-access port-mac-filter	Enables the specified MAC address filter	IC
mac-authentication intrusion-action	Determines the port response when a connected host fails MAC authentication.	IC
mac-authentication max-mac-count	Sets the maximum number of MAC addresses that can be authenticated on a port via MAC authentication	IC
clear network-access mac-address-table	Clears authenticated MAC addresses from the address table	PE
show network-access	Displays the MAC authentication settings for port interfaces	PE
show network-access mac-address-table	Displays information for entries in the secure MAC address table	PE
show network-access mac-filter	Displays information for entries in the MAC filter tables	PE

network-access aging

Use this command to enable aging for authenticated MAC addresses stored in the secure MAC address table. Use the **no** form of this command to disable address aging.

SYNTAX

[**no**] **network-access aging**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- Authenticated MAC addresses are stored as dynamic entries in the switch's secure MAC address table and are removed when the aging time expires. The address aging time is determined by the mac-address-table aging-time command.
- This parameter applies to authenticated MAC addresses configured by the MAC Address Authentication process described in this section, as well as to any secure MAC addresses authenticated by 802.1X, regardless of the 802.1X Operation Mode (Single-Host, Multi-Host, or MAC-Based authentication as described on page 593).
- The maximum number of secure MAC addresses supported for the switch system is 1024.

EXAMPLE

```
Console(config-if)#network-access aging
Console(config-if)#
```

network-access mac-filter

Use this command to add a MAC address into a filter table. Use the **no** form of this command to remove the specified MAC address.

SYNTAX

[**no**] **network-access mac-filter** *filter-id*
mac-address *mac-address* [**mask** *mask-address*]

filter-id - Specifies a MAC address filter table. (Range: 1-64)

mac-address - Specifies a MAC address entry.
(Format: xx-xx-xx-xx-xx-xx)

mask - Specifies a MAC address bit mask for a range of addresses.

DEFAULT SETTING

Disabled

COMMAND MODE
Global Configuration

COMMAND USAGE
- Specified addresses are exempt from network access authentication.
- This command is different from configuring static addresses with the mac-address-table static command in that it allows you configure a range of addresses when using a mask, and then to assign these addresses to one or more ports with the network-access port-mac-filter command.
- Up to 64 filter tables can be defined.
- There is no limitation on the number of entries that can entered in a filter table.

EXAMPLE

```
Console(config)#network-access mac-filter 1 mac-address 11-22-33-44-55-66
Console(config)#
```

mac-authentication reauth-time

Use this command to set the time period after which a connected MAC address must be re-authenticated. Use the **no** form of this command to restore the default value.

SYNTAX

mac-authentication reauth-time *seconds*

no mac-authentication reauth-time

seconds - The reauthentication time period. (Range: 120-1000000 seconds)

DEFAULT SETTING
1800

COMMAND MODE
Global Configuration

COMMAND USAGE
- The reauthentication time is a global setting and applies to all ports.
- When the reauthentication time expires for a secure MAC address it is reauthenticated with the RADIUS server. During the reauthentication process traffic through the port remains unaffected.

EXAMPLE

```
Console(config)#mac-authentication reauth-time 300
Console(config)#
```

network-access dynamic-qos

Use this command to enable the dynamic QoS feature for an authenticated port. Use the **no** form to restore the default.

SYNTAX

[**no**] **network-access dynamic-qos**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration

COMMAND USAGE

- The RADIUS server may optionally return dynamic QoS assignments to be applied to a switch port for an authenticated user. The "Filter-ID" attribute (attribute 11) can be configured on the RADIUS server to pass the following QoS information:

Table 79: Dynamic QoS Profiles

Profile	Attribute Syntax	Example
DiffServ	**service-policy-in**=*policy-map-name*	service-policy-in=p1
Rate Limit	**rate-limit-input**=*rate*	rate-limit-input=100 (Kbps)
802.1p	**switchport-priority-default**=*value*	switchport-priority-default=2

- When the last user logs off of a port with a dynamic QoS assignment, the switch restores the original QoS configuration for the port.
- When a user attempts to log into the network with a returned dynamic QoS profile that is different from users already logged on to the same port, the user is denied access.
- While a port has an assigned dynamic QoS profile, any manual QoS configuration changes only take effect after all users have logged off of the port.

NOTE: Any configuration changes for dynamic QoS are not saved to the switch configuration file.

EXAMPLE

The following example enables the dynamic QoS feature on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access dynamic-qos
Console(config-if)#
```

network-access dynamic-vlan

Use this command to enable dynamic VLAN assignment for an authenticated port. Use the **no** form to disable dynamic VLAN assignment.

SYNTAX

[**no**] **network-access dynamic-vlan**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration

COMMAND USAGE

- When enabled, the VLAN identifiers returned by the RADIUS server will be applied to the port, providing the VLANs have already been created on the switch. GVRP is not used to create the VLANs.
- The VLAN settings specified by the first authenticated MAC address are implemented for a port. Other authenticated MAC addresses on the port must have same VLAN configuration, or they are treated as an authentication failure.
- If dynamic VLAN assignment is enabled on a port and the RADIUS server returns no VLAN configuration, the authentication is still treated as a success, and the host assigned to the default untagged VLAN.
- When the dynamic VLAN assignment status is changed on a port, all authenticated addresses are cleared from the secure MAC address table.

EXAMPLE

The following example enables dynamic VLAN assignment on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access dynamic-vlan
Console(config-if)#
```

network-access guest-vlan

Use this command to assign all traffic on a port to a guest VLAN when network access (MAC authentication) or 802.1x authentication is rejected. Use the **no** form of this command to disable guest VLAN assignment.

SYNTAX

network-access guest-vlan *vlan-id*

no network-access guest-vlan

vlan-id - VLAN ID (Range: 1-4094)

DEFAULT SETTING

Disabled

COMMAND MODE
Interface Configuration

COMMAND USAGE
- The VLAN to be used as the guest VLAN must be defined and set as active (See the vlan database command).
- When used with 802.1X authentication, the intrusion-action must be set for "guest-vlan" to be effective (see the dot1x intrusion-action command).

EXAMPLE
```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access guest-vlan 25
Console(config-if)#
```

network-access link-detection

Use this command to enable link detection for the selected port. Use the **no** form of this command to restore the default.

SYNTAX
[**no**] **network-access link-detection**

DEFAULT SETTING
Disabled

COMMAND MODE
Interface Configuration

EXAMPLE
```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection
Console(config-if)#
```

network-access link-detection link-down

Use this command to detect link-down events. When detected, the switch can shut down the port, send an SNMP trap, or both. Use the **no** form of this command to disable this feature.

SYNTAX

network-access link-detection link-down
action [**shutdown** | **trap** | **trap-and-shutdown**]

no network-access link-detection

action - Response to take when port security is violated.

shutdown - Disable port only.

trap - Issue SNMP trap message only.

trap-and-shutdown - Issue SNMP trap message and disable the port.

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection link-down action trap
Console(config-if)#
```

network-access link-detection link-up

Use this command to detect link-up events. When detected, the switch can shut down the port, send an SNMP trap, or both. Use the **no** form of this command to disable this feature.

SYNTAX

network-access link-detection link-up
action [**shutdown** | **trap** | **trap-and-shutdown**]

no network-access link-detection

action - Response to take when port security is violated.

shutdown - Disable port only.

trap - Issue SNMP trap message only.

trap-and-shutdown - Issue SNMP trap message and disable the port.

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection link-up action trap
Console(config-if)#
```

network-access link-detection link-up-down

Use this command to detect link-up and link-down events. When either event is detected, the switch can shut down the port, send an SNMP trap, or both. Use the **no** form of this command to disable this feature.

SYNTAX

network-access link-detection link-up-down
action [**shutdown** | **trap** | **trap-and-shutdown**]

no network-access link-detection

action - Response to take when port security is violated.

shutdown - Disable port only.

trap - Issue SNMP trap message only.

trap-and-shutdown - Issue SNMP trap message and disable the port.

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection link-up-down action trap
Console(config-if)#
```

network-access max-mac-count

Use this command to set the maximum number of MAC addresses that can be authenticated on a port interface via all forms of authentication. Use the **no** form of this command to restore the default.

SYNTAX

network-access max-mac-count *count*

no network-access max-mac-count

count - The maximum number of authenticated IEEE 802.1X and MAC addresses allowed. (Range: 0-1024; 0 for unlimited)

DEFAULT SETTING

1024

COMMAND MODE
Interface Configuration

COMMAND USAGE
The maximum number of MAC addresses per port is 1024, and the maximum number of secure MAC addresses supported for the switch system is 1024. When the limit is reached, all new MAC addresses are treated as authentication failed.

EXAMPLE

```
Console(config-if)#network-access max-mac-count 5
Console(config-if)#
```

network-access mode mac-authentication

Use this command to enable network access authentication on a port. Use the **no** form of this command to disable network access authentication.

SYNTAX

[**no**] **network-access mode mac-authentication**

DEFAULT SETTING
Disabled

COMMAND MODE
Interface Configuration

COMMAND USAGE
- When enabled on a port, the authentication process sends a Password Authentication Protocol (PAP) request to a configured RADIUS server. The user name and password are both equal to the MAC address being authenticated.
- On the RADIUS server, PAP user name and passwords must be configured in the MAC address format XX-XX-XX-XX-XX-XX (all in upper case).
- Authenticated MAC addresses are stored as dynamic entries in the switch secure MAC address table and are removed when the aging time expires. The maximum number of secure MAC addresses supported for the switch system is 1024.
- Configured static MAC addresses are added to the secure address table when seen on a switch port. Static addresses are treated as authenticated without sending a request to a RADIUS server.
- MAC authentication, 802.1X, and port security cannot be configured together on the same port. Only one security mechanism can be applied.
- MAC authentication cannot be configured on trunk ports.

- When port status changes to down, all MAC addresses are cleared from the secure MAC address table. Static VLAN assignments are not restored.
- The RADIUS server may optionally return a VLAN identifier list. VLAN identifier list is carried in the "Tunnel-Private-Group-ID" attribute. The VLAN list can contain multiple VLAN identifiers in the format "1u,2t," where "u" indicates untagged VLAN and "t" tagged VLAN. The "Tunnel-Type" attribute should be set to "VLAN," and the "Tunnel-Medium-Type" attribute set to "802."

EXAMPLE

```
Console(config-if)#network-access mode mac-authentication
Console(config-if)#
```

network-access port-mac-filter

Use this command to enable the specified MAC address filter. Use the **no** form of this command to disable the specified MAC address filter.

SYNTAX

network-access port-mac-filter *filter-id*

no network-access port-mac-filter

filter-id - Specifies a MAC address filter table. (Range: 1-64)

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration

COMMAND MODE

- Entries in the MAC address filter table can be configured with the network-access mac-filter command.
- Only one filter table can be assigned to a port.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access port-mac-filter 1
Console(config-if)#
```

mac-authentication intrusion-action

Use this command to configure the port response to a host MAC authentication failure. Use the **no** form of this command to restore the default.

SYNTAX

mac-authentication intrusion-action {**block traffic** | **pass traffic**}

no mac-authentication intrusion-action

DEFAULT SETTING

Block Traffic

COMMAND MODE

Interface Con figuration

EXAMPLE

```
Console(config-if)#mac-authentication intrusion-action block-traffic
Console(config-if)#
```

mac-authentication max-mac-count

Use this command to set the maximum number of MAC addresses that can be authenticated on a port via MAC authentication. Use the **no** form of this command to restore the default.

SYNTAX

mac-authentication max-mac-count *count*

no mac-authentication max-mac-count

count - The maximum number of MAC-authenticated MAC addresses allowed. (Range: 1-1024)

DEFAULT SETTING

1024

COMMAND MODE

Interface Configuration

EXAMPLE

```
Console(config-if)#mac-authentication max-mac-count 32
Console(config-if)#
```

clear network-access mac-address-table

Use this command to clear entries from the secure MAC addresses table.

SYNTAX

clear network-access mac-address-table [**static** | **dynamic**] [**address** *mac-address*] [**interface** *interface*]

static - Specifies static address entries.

dynamic - Specifies dynamic address entries.

mac-address - Specifies a MAC address entry. (Format: xx-xx-xx-xx-xx-xx)

interface - Specifies a port interface.

ethernet *unit*/*port*

unit - This is unit 1.

port - Port number. (Range: 1-28/52)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#clear network-access mac-address-table interface ethernet 1/1
Console#
```

show network-access

Use this command to display the MAC authentication settings for port interfaces.

SYNTAX

show network-access [**interface** *interface*]

interface - Specifies a port interface.

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

DEFAULT SETTING

Displays the settings for all interfaces.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show network-access interface ethernet 1/1
Global secure port information
Reauthentication Time                 : 1800
-------------------------------------------------
-------------------------------------------------
Port : 1/1
MAC Authentication                    : Disabled
MAC Authentication Intrusion action   : Block traffic
MAC Authentication Maximum MAC Counts : 1024
Maximum MAC Counts                    : 2048
Dynamic VLAN Assignment               : Enabled
Dynamic QoS Assignment                : Disabled
MAC Filter ID                         : Disabled
Guest VLAN                            : Disabled
Link Detection                        : Disabled
Detection Mode                        : Link-down
Detection Action                      : Shutdown
Console#
```

show network-access mac-address-table

Use this command to display secure MAC address table entries.

SYNTAX

show network-access mac-address-table [**static** | **dynamic**] [**address** *mac-address* [*mask*]] [**interface** *interface*] [**sort** {**address** | **interface**}]

static - Specifies static address entries.

dynamic - Specifies dynamic address entries.

mac-address - Specifies a MAC address entry. (Format: xx-xx-xx-xx-xx-xx)

mask - Specifies a MAC address bit mask for filtering displayed addresses.

interface - Specifies a port interface.

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

sort - Sorts displayed entries by either MAC address or interface.

DEFAULT SETTING

Displays all filters.

COMMAND MODE

Privileged Exec

COMMAND USAGE

When using a bit mask to filter displayed MAC addresses, a 1 means “care” and a 0 means “don't care”. For example, a MAC of 00-00-01-02-03-04 and mask FF-FF-FF-00-00-00 would result in all MACs in the range 00-00-01-

00-00-00 to 00-00-01-FF-FF-FF to be displayed. All other MACs would be filtered out.

EXAMPLE

```
Console#show network-access mac-address-table
Interface MAC Address       RADIUS Server   Time                      Attribute
--------- ----------------- --------------- ------------------------- ---------
Eth 1/ 1  00-E0-29-94-34-64         0.0.0.0 2001y 01m 01d 05h 57m 43s Static
Eth 1/ 1  00-00-01-02-03-04  172.155.120.17 2001y 01m 00d 06h 32m 50s Static
Eth 1/ 1  00-00-01-02-03-05  172.155.120.17 2001y 01m 00d 06h 33m 20s Dynamic
Eth 1/ 1  00-00-01-02-03-06  172.155.120.17 2001y 01m 00d 06h 35m 10s Static
Eth 1/ 3  00-00-01-02-03-07  172.155.120.17 2001y 01m 00d 06h 34m 20s Dynamic

Console#
```

show network-access mac-filter

Use this command to display information for entries in the MAC filter tables.

SYNTAX

show network-access mac-filter [*filter-id*]

filter-id - Specifies a MAC address filter table. (Range: 1-64)

DEFAULT SETTING

Displays all filters.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show network-access mac-filter
Filter ID MAC Address       MAC Mask
--------- ----------------- -----------------
        1 00-00-01-02-03-08 FF-FF-FF-FF-FF-FF
Console#
```

WEB AUTHENTICATION

Web authentication allows stations to authenticate and access the network in situations where 802.1X or Network Access authentication are infeasible or impractical. The web authentication feature allows unauthenticated hosts to request and receive a DHCP assigned IP address and perform DNS queries. All other traffic, except for HTTP protocol traffic, is blocked. The switch intercepts HTTP protocol traffic and redirects it to a switch-generated web page that facilitates user name and password authentication via RADIUS. Once authentication is successful, the web browser is forwarded on to the originally requested web page. Successful authentication is valid for all hosts connected to the port.

NOTE: RADIUS authentication must be activated and configured for the web authentication feature to work properly (see "Authentication Sequence").

NOTE: Web authentication cannot be configured on trunk ports.

Table 80: Web Authentication

Command	Function	Mode
web-auth login-attempts	Defines the limit for failed web authentication login attempts	GC
web-auth quiet-period	Defines the amount of time to wait after the limit for failed login attempts is exceeded.	GC
web-auth session-timeout	Defines the amount of time a session remains valid	GC
web-auth system-auth-control	Enables web authentication globally for the switch	GC
web-auth	Enables web authentication for an interface	IC
web-auth re-authenticate (Port)	Ends all web authentication sessions on the port and forces the users to re-authenticate	PE
web-auth re-authenticate (IP)	Ends the web authentication session associated with the designated IP address and forces the user to re-authenticate	PE
show web-auth	Displays global web authentication parameters	PE
show web-auth interface	Displays interface-specific web authentication parameters and statistics	PE
show web-auth summary	Displays a summary of web authentication port parameters and statistics	PE

web-auth login-attempts

This command defines the limit for failed web authentication login attempts. After the limit is reached, the switch refuses further login attempts until the quiet time expires. Use the **no** form to restore the default.

SYNTAX

web-auth login-attempts *count*

no web-auth login-attempts

count - The limit of allowed failed login attempts. (Range: 1-3)

DEFAULT SETTING

3 login attempts

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#web-auth login-attempts 2
Console(config)#
```

web-auth quiet-period

This command defines the amount of time a host must wait after exceeding the limit for failed login attempts, before it may attempt web authentication again. Use the **no** form to restore the default.

SYNTAX

web-auth quiet-period *time*

no web-auth quiet period

time - The amount of time the host must wait before attempting authentication again. (Range: 1-180 seconds)

DEFAULT SETTING

60 seconds

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#web-auth quiet-period 120
Console(config)#
```

web-auth session-timeout

This command defines the amount of time a web-authentication session remains valid. When the session timeout has been reached, the host is logged off and must re-authenticate itself the next time data transmission takes place. Use the **no** form to restore the default.

SYNTAX

web-auth session-timeout *timeout*

no web-auth session timeout

timeout - The amount of time that an authenticated session remains valid. (Range: 300-3600 seconds)

DEFAULT SETTING

3600 seconds

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#web-auth session-timeout 1800
Console(config)#
```

web-auth system-auth-control

This command globally enables web authentication for the switch. Use the **no** form to restore the default.

SYNTAX

[**no**] **web-auth system-auth-control**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

Both **web-auth system-auth-control** for the switch and web-auth for an interface must be enabled for the web authentication feature to be active.

EXAMPLE

```
Console(config)#web-auth system-auth-control
Console(config)#
```

web-auth

This command enables web authentication for an interface. Use the no form to restore the default.

SYNTAX

[**no**] **web-auth**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration

COMMAND USAGE

Both web-auth system-auth-control for the switch and **web-auth** for a port must be enabled for the web authentication feature to be active.

EXAMPLE

```
Console(config-if)#web-auth
Console(config-if)#
```

web-auth re-authenticate (Port)

This command ends all web authentication sessions connected to the port and forces the users to re-authenticate.

SYNTAX

web-auth re-authenticate interface *interface*

interface - Specifies a port interface.

ethernet *unit*/*port*

unit - This is unit 1.

port - Port number. (Range: 1-28/52)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#web-auth re-authenticate interface ethernet 1/2
Failed to reauth.
Console#
```

web-auth re-authenticate (IP)

This command ends the web authentication session associated with the designated IP address and forces the user to re-authenticate.

SYNTAX

web-auth re-authenticate interface *interface ip*

interface - Specifies a port interface.

ethernet *unit*/*port*

unit - This is unit 1.

port - Port number. (Range: 1-28/52)

ip - IPv4 formatted IP address

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#web-auth re-authenticate interface ethernet 1/2 192.168.1.5
Failed to reauth port.
Console#
```

show web-auth

This command displays global web authentication parameters.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show web-auth

Global Web-Auth Parameters

  System Auth Control      : Enabled
  Session Timeout          : 3600
  Quiet Period             : 60
  Max Login Attempts       : 3
Console#
```

show web-auth interface

This command displays interface-specific web authentication parameters and statistics.

SYNTAX

show web-auth interface *interface*

interface - Specifies a port interface.

ethernet *unit*/*port*

unit - This is unit 1.

port - Port number. (Range: 1-28/52)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#
Web Auth Status      : Enabled

Host Summary

IP address      Web-Auth-State Remaining-Session-Time
--------------- -------------- ----------------------
1.1.1.1         Authenticated  295
1.1.1.2         Authenticated  111
Console#
```

show web-auth summary

This command displays a summary of web authentication port parameters and statistics.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show web-auth summary

Global Web-Auth Parameters

  System Auth Control      : Enabled
Port       Status         Authenticated Host Count
----       ------         ------------------------
1/ 1       Disabled       0
1/ 2       Enabled        8
1/ 3       Disabled       0
1/ 4       Disabled       0
1/ 5       Disabled       0
⋮
```

DHCP SNOOPING

DHCP snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port. This section describes commands used to configure DHCP snooping.

Table 81: DHCP Snooping Commands

Command	Function	Mode
ip dhcp snooping	Enables DHCP snooping globally	GC
ip dhcp snooping information option	Enables or disables DHCP Option 82 information relay	GC
ip dhcp snooping information policy	Sets the information option policy for DHCP client packets that include Option 82 information	GC
ip dhcp snooping verify mac-address	Verifies the client's hardware address stored in the DHCP packet against the source MAC address in the Ethernet header	GC
ip dhcp snooping vlan	Enables DHCP snooping on the specified VLAN	GC
ip dhcp snooping trust	Configures the specified interface as trusted	IC
clear ip dhcp snooping database flash	Removes all dynamically learned snooping entries from flash memory.	PE
ip dhcp snooping database flash	Writes all dynamically learned snooping entries to flash memory	PE
show ip dhcp snooping	Shows the DHCP snooping configuration settings	PE
show ip dhcp snooping binding	Shows the DHCP snooping binding table entries	PE

ip dhcp snooping

This command enables DHCP snooping globally. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **ip dhcp snooping**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- Network traffic may be disrupted when malicious DHCP messages are received from an outside source. DHCP snooping is used to filter DHCP messages received on an unsecure interface from outside the network or fire wall. When DHCP snooping is enabled globally by this command, and enabled on a VLAN interface by the ip dhcp snooping vlan command, DHCP messages received on an untrusted interface (as specified by the no ip dhcp snooping trust command) from a device not listed in the DHCP snooping table will be dropped.

- When enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.

- Table entries are only learned for trusted interfaces. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier.

- When DHCP snooping is enabled, the rate limit for the number of DHCP messages that can be processed by the switch is 100 packets per second. Any DHCP packets in excess of this limit are dropped.

- Filtering rules are implemented as follows:

  - If the global DHCP snooping is disabled, all DHCP packets are forwarded.

  - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a *trusted* port. If the received packet is a DHCP ACK message, a dynamic DHCP snooping entry is also added to the binding table.

  - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is *not trusted*, it is processed as follows:

    - If the DHCP packet is a reply packet from a DHCP server (including OFFER, ACK or NAK messages), the packet is dropped.

- If the DHCP packet is from a client, such as a DECLINE or RELEASE message, the switch forwards the packet only if the corresponding entry is found in the binding table.
- If the DHCP packet is from client, such as a DISCOVER, REQUEST, INFORM, DECLINE or RELEASE message, the packet is forwarded if MAC address verification is disabled (as specified by the ip dhcp snooping verify mac-address command). However, if MAC address verification is enabled, then the packet will only be forwarded if the client's hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.
- If the DHCP packet is not a recognizable type, it is dropped.

- If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.
- If a DHCP packet is from server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.

- If the DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.
- *Additional considerations when the switch itself is a DHCP client* – The port(s) through which the switch submits a client request to the DHCP server must be configured as trusted (using the ip dhcp snooping trust command). Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCP server. Also, when the switch sends out DHCP client packets for itself, no filtering takes place. However, when the switch receives any messages from a DHCP server, any packets received from untrusted ports are dropped.

EXAMPLE

This example enables DHCP snooping globally for the switch.

```
Console(config)#ip dhcp snooping
Console(config)#
```

RELATED COMMANDS

ip dhcp snooping vlan (640)
ip dhcp snooping trust (641)

ip dhcp snooping information option

This command enables the DHCP Option 82 information relay for the switch. Use the **no** form to disable this function.

SYNTAX

[**no**] **ip dhcp snooping information option**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- DHCP provides a relay mechanism for sending information about the switch and its DHCP clients to the DHCP server. Known as DHCP Option 82, it allows compatible DHCP servers to use the information when assigning IP addresses, or to set other services or policies for clients.
- When the DHCP Snooping Information Option is enabled, the requesting client (or an intermediate relay agent that has used the information fields to describe itself) can be identified in the DHCP request packets forwarded by the switch and in reply packets sent back from the DHCP server by the switch port to which they are connected rather than just their MAC address. DHCP client-server exchange messages are then forwarded directly between the server and client without having to flood them to the entire VLAN.
- DHCP snooping must be enabled on the switch for the DHCP Option 82 information to be inserted into packets.
- Use the **ip dhcp snooping information option** command to specify how to handle DHCP client request packets which already contain Option 82 information.

EXAMPLE

This example enables the DHCP Snooping Information Option.

```
Console(config)#ip dhcp snooping information option
Console(config)#
```

ip dhcp snooping information policy

This command sets the DHCP snooping information option policy for DHCP client packets that include Option 82 information.

SYNTAX

ip dhcp snooping information policy {**drop** | **keep** | **replace**}

drop - Drops the client's request packet instead of relaying it.

keep - Retains the Option 82 information in the client request, and forwards the packets to trusted ports.

replace - Replaces the Option 82 information circuit-id and remote-id fields in the client's request with information about the relay agent itself, inserts the relay agent's address (when DHCP snooping is enabled), and forwards the packets to trusted ports.

DEFAULT SETTING

replace

COMMAND MODE

Global Configuration

COMMAND USAGE

When the switch receives DHCP packets from clients that already include DHCP Option 82 information, the switch can be configured to set the action policy for these packets. The switch can either drop the DHCP packets, keep the existing information, or replace it with the switch's relay information.

EXAMPLE

```
Console(config)#ip dhcp snooping information policy drop
Console(config)#
```

ip dhcp snooping verify mac-address

This command verifies the client's hardware address stored in the DHCP packet against the source MAC address in the Ethernet header. Use the **no** form to disable this function.

SYNTAX

[**no**] **ip dhcp binding verify mac-address**

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

COMMAND USAGE

If MAC address verification is enabled, and the source MAC address in the Ethernet header of the packet is not same as the client's hardware address in the DHCP packet, the packet is dropped.

EXAMPLE

This example enables MAC address verification.

```
Console(config)#ip dhcp snooping verify mac-address
Console(config)#
```

RELATED COMMANDS

ip dhcp snooping (636)
ip dhcp snooping vlan (640)
ip dhcp snooping trust (641)

ip dhcp snooping vlan

This command enables DHCP snooping on the specified VLAN. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **ip dhcp snooping vlan** *vlan-id*

vlan-id - ID of a configured VLAN (Range: 1-4094)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- When DHCP snooping enabled globally using the ip dhcp snooping command, and enabled on a VLAN with this command, DHCP packet filtering will be performed on any untrusted ports within the VLAN as specified by the ip dhcp snooping trust command.
- When the DHCP snooping is globally disabled, DHCP snooping can still be configured for specific VLANs, but the changes will not take effect until DHCP snooping is globally re-enabled.
- When DHCP snooping is globally enabled, configuration changes for specific VLANs have the following effects:
  - If DHCP snooping is disabled on a VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.

EXAMPLE

This example enables DHCP snooping for VLAN 1.

```
Console(config)#ip dhcp snooping vlan 1
Console(config)#
```

RELATED COMMANDS

ip dhcp snooping (636)
ip dhcp snooping trust (641)

ip dhcp snooping trust

This command configures the specified interface as trusted. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **ip dhcp snooping trust**

DEFAULT SETTING

All interfaces are untrusted

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- A trusted interface is an interface that is configured to receive only messages from within the network. An untrusted interface is an interface that is configured to receive messages from outside the network or fire wall.
- Set all ports connected to DHCP servers within the local network or fire wall to trusted, and all other ports outside the local network or fire wall to untrusted.
- When DHCP snooping ia enabled globally using the ip dhcp snooping command, and enabled on a VLAN with ip dhcp snooping vlan command, DHCP packet filtering will be performed on any untrusted ports within the VLAN according to the default status, or as specifically configured for an interface with the **no ip dhcp snooping trust** command.
- When an untrusted port is changed to a trusted port, all the dynamic DHCP snooping bindings associated with this port are removed.
- *Additional considerations when the switch itself is a DHCP client* – The port(s) through which it submits a client request to the DHCP server must be configured as trusted.

EXAMPLE

This example sets port 5 to untrusted.

```
Console(config)#interface ethernet 1/5
Console(config-if)#no ip dhcp snooping trust
Console(config-if)#
```

RELATED COMMANDS

ip dhcp snooping (636)
ip dhcp snooping vlan (640)

clear ip dhcp snooping database flash

This command removes all dynamically learned snooping entries from flash memory.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console(config)#ip dhcp snooping database flash
Console(config)#
```

ip dhcp snooping database flash

This command writes all dynamically learned snooping entries to flash memory.

COMMAND MODE

Privileged Exec

COMMAND USAGE

This command can be used to store the currently learned dynamic DHCP snooping entries to flash memory. These entries will be restored to the snooping table when the switch is reset. However, note that the lease time shown for a dynamic entry that has been restored from flash memory will no longer be valid.

EXAMPLE

```
Console(config)#ip dhcp snooping database flash
Console(config)#
```

show ip dhcp snooping

This command shows the DHCP snooping configuration settings.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip dhcp snooping
Global DHCP Snooping status: disable
DHCP Snooping Information Option Status: disable
DHCP Snooping Information Option Remote ID: mac address
DHCP Snooping Information Policy: replace
DHCP Snooping is configured on the following VLANs:
1
Verify Source Mac-Address: enable
Interface           Trusted
----------          ----------
Eth 1/1             No
Eth 1/2             No
Eth 1/3             No
Eth 1/4             No
Eth 1/5             Yes
.
.
.
```

show ip dhcp snooping binding

This command shows the DHCP snooping binding table entries.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip dhcp snooping binding
MacAddress        IpAddress       Lease(sec) Type                VLAN Interface
----------------- --------------- ---------- -------------------- ---- ------
11-22-33-44-55-66 192.168.0.99             0 Dynamic-DHCPSNP         1 Eth 1/5
Console#
```

IP SOURCE GUARD

IP Source Guard is a security feature that filters IP traffic on network interfaces based on manually configured entries in the IP Source Guard table, or dynamic entries in the DHCP Snooping table when enabled (see "DHCP Snooping"). IP source guard can be used to prevent traffic attacks caused when a host tries to use the IP address of a neighbor to access the network. This section describes commands used to configure IP Source Guard.

Table 82: IP Source Guard Commands

Command	Function	Mode
ip source-guard binding	Adds a static address to the source-guard binding table	GC
ip source-guard	Configures the switch to filter inbound traffic based on source IP address, or source IP address and corresponding MAC address	IC
ip source-guard max-binding	Sets the maximum number of entries that can be bound to an interface	IC
show ip source-guard	Shows whether source guard is enabled or disabled on each interface	PE
show ip source-guard binding	Shows the source guard binding table	PE

ip source-guard binding

This command adds a static address to the source-guard binding table. Use the **no** form to remove a static entry.

SYNTAX

ip source-guard binding *mac-address* **vlan** *vlan-id ip-address* **interface ethernet** *unit/port*

no ip source-guard binding *mac-address* **vlan** *vlan-id*

mac-address - A valid unicast MAC address.

vlan-id - ID of a configured VLAN (Range: 1-4094)

ip-address - A valid unicast IP address, including classful types A, B or C.

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

DEFAULT SETTING

No configured entries

COMMAND MODE

Global Configuration

COMMAND USAGE

- Table entries include a MAC address, IP address, lease time, entry type (Static-IP-SG-Binding, Dynamic-DHCP-Binding), VLAN identifier, and port identifier.
- All static entries are configured with an infinite lease time, which is indicated with a value of zero by the show ip source-guard command.
- When source guard is enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping, or static addresses configured in the source guard binding table with this command.
- Static bindings are processed as follows:
  - If there is no entry with same VLAN ID and MAC address, a new entry is added to binding table using the type of static IP source guard binding.
  - If there is an entry with same VLAN ID and MAC address, and the type of entry is static IP source guard binding, then the new entry will replace the old one.
  - If there is an entry with same VLAN ID and MAC address, and the type of the entry is dynamic DHCP snooping binding, then the new entry will replace the old one and the entry type will be changed to static IP source guard binding.

EXAMPLE

This example configures a static source-guard binding on port 5.

```
Console(config)#ip source-guard binding 11-22-33-44-55-66 vlan 1 192.168.0.99
  interface ethernet 1/5
Console(config-if)#
```

RELATED COMMANDS

ip source-guard (646)
ip dhcp snooping (636)
ip dhcp snooping vlan (640)

ip source-guard

This command configures the switch to filter inbound traffic based source IP address, or source IP address and corresponding MAC address. Use the **no** form to disable this function.

SYNTAX

ip source-guard {**sip** | **sip-mac**}

no ip source-guard

sip - Filters traffic based on IP addresses stored in the binding table.

sip-mac - Filters traffic based on IP addresses and corresponding MAC addresses stored in the binding table.

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- Source guard is used to filter traffic on an insecure port which receives messages from outside the network or fire wall, and therefore may be subject to traffic attacks caused by a host trying to use the IP address of a neighbor.
- Setting source guard mode to "sip" or "sip-mac" enables this function on the selected port. Use the "sip" option to check the VLAN ID, source IP address, and port number against all entries in the binding table. Use the "sip-mac" option to check these same parameters, plus the source MAC address. Use the **no ip source guard** command to disable this function on the selected port.
- When enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping, or static addresses configured in the source guard binding table.
- Table entries include a MAC address, IP address, lease time, entry type (Static-IP-SG-Binding, Dynamic-DHCP-Binding, VLAN identifier, and port identifier.
- Static addresses entered in the source guard binding table with the ip source-guard binding command are automatically configured with an infinite lease time. Dynamic entries learned via DHCP snooping are configured by the DHCP server itself.
- If the IP source guard is enabled, an inbound packet's IP address (sip option) or both its IP address and corresponding MAC address (sip-mac option) will be checked against the binding table. If no matching entry is found, the packet will be dropped.

- Filtering rules are implemented as follows:
  - If DHCP snooping is disabled (see page 636), IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the sip-mac option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, the packet will be forwarded.
  - If the DHCP snooping is enabled, IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the sip-mac option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, or dynamic DHCP snooping binding, the packet will be forwarded.
  - If IP source guard if enabled on an interface for which IP source bindings (dynamically learned via DHCP snooping or manually configured) are not yet configured, the switch will drop all IP traffic on that port, except for DHCP packets.
  - Only unicast addresses are accepted for static bindings.

EXAMPLE

This example enables IP source guard on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard sip
Console(config-if)#
```

RELATED COMMANDS

ip source-guard binding (644)
ip dhcp snooping (636)
ip dhcp snooping vlan (640)

ip source-guard max-binding

This command sets the maximum number of entries that can be bound to an interface. Use the **no** form to restore the default setting.

SYNTAX

ip source-guard max-binding *number*

no ip source-guard max-binding

number - The maximum number of IP addresses that can be mapped to an interface in the binding table. (Range: 1-16)

DEFAULT SETTING

16

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- This command sets the maximum number of address entries that can be mapped to an interface in the binding table, including both dynamic entries discovered by DHCP snooping and static entries set by the ip source-guard command.

EXAMPLE

This example sets the maximum number of allowed entries in the binding table for port 5 to one entry.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard max-binding 1
Console(config-if)#
```

show ip source-guard

This command shows whether source guard is enabled or disabled on each interface.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip source-guard
Interface   Filter-type   Max-binding
---------   -----------   -----------
Eth 1/ 1    DISABLED               16
Eth 1/ 2    DISABLED               16
Eth 1/ 3    DISABLED               16
Eth 1/ 4    DISABLED               16
Eth 1/5     SIP                     1
Eth 1/6     DISABLED               16
⋮
```

show ip source-guard binding

This command shows the source guard binding table.

SYNTAX

show ip source-guard binding [**dhcp-snooping** | **static**]

dhcp-snooping - Shows dynamic entries configured with DHCP Snooping commands (see page 635)

static - Shows static entries configured with the ip source-guard binding command.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip source-guard binding
MacAddress        IpAddress       Lease(sec) Type                VLAN Interface
----------------- --------------- ---------- -------------------- ---- ---------
11-22-33-44-55-66 192.168.0.99             0 Static                1 Eth 1/5
Console#
```

ARP INSPECTION

ARP Inspection validates the MAC-to-IP address bindings in Address Resolution Protocol (ARP) packets. It protects against ARP traffic with invalid address bindings, which forms the basis for certain "man-in-the-middle" attacks. This is accomplished by intercepting all ARP requests and responses and verifying each of these packets before the local ARP cache is updated or the packet is forwarded to the appropriate destination, dropping any invalid ARP packets.

ARP Inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database – the DHCP snooping binding database. ARP Inspection can also validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured IP addresses.

This section describes commands used to configure ARP Inspection.

Table 83: ARP Inspection Commands

Command	Function	Mode
ip arp inspection	Enables ARP Inspection globally on the switch	GC
ip arp inspection filter	Specifies an ARP ACL to apply to one or more VLANs	GC
ip arp inspection log-buffer logs	Sets the maximum number of entries saved in a log message, and the rate at these messages are sent	GC
ip arp inspection validate	Specifies additional validation of address components in an ARP packet	GC
ip arp inspection vlan	Enables ARP Inspection for a specified VLAN or range of VLANs	GC
ip arp inspection limit	Sets a rate limit for the ARP packets received on a port	IC
ip arp inspection trust	Sets a port as trusted, and thus exempted from ARP Inspection	IC
show ip arp inspection configuration	Displays the global configuration settings for ARP Inspection	PE
show ip arp inspection interface	Shows the trust status and inspection rate limit for ports	PE
show ip arp inspection log	Shows information about entries stored in the log, including the associated VLAN, port, and address components	PE

Table 83: ARP Inspection Commands (Continued)

Command	Function	Mode
show ip arp inspection statistics	Shows statistics about the number of ARP packets processed, or dropped for various reasons	PE
show ip arp inspection vlan	Shows configuration setting for VLANs, including ARP Inspection status, the ARP ACL name, and if the DHCP Snooping database is used after ACL validation is completed	PE

ip arp inspection

This command enables ARP Inspection globally on the switch. Use the **no** form to disable this function.

SYNTAX

[**no**] **ip arp inspection**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- When ARP Inspection is enabled globally with this command, it becomes active only on those VLANs where it has been enabled with the ip arp inspection vlan command.
- When ARP Inspection is enabled globally and enabled on selected VLANs, all ARP request and reply packets on those VLANs are redirected to the CPU and their switching is handled by the ARP Inspection engine.
- When ARP Inspection is disabled globally, it becomes inactive for all VLANs, including those where ARP Inspection is enabled.
- When ARP Inspection is disabled, all ARP request and reply packets bypass the ARP Inspection engine and their manner of switching matches that of all other packets.
- Disabling and then re-enabling global ARP Inspection will not affect the ARP Inspection configuration for any VLANs.
- When ARP Inspection is disabled globally, it is still possible to configure ARP Inspection for individual VLANs. These configuration changes will only become active after ARP Inspection is globally enabled again.

EXAMPLE

```
Console(config)#ip arp inspection
Console(config)#
```

ip arp inspection filter

This command specifies an ARP ACL to apply to one or more VLANs. Use the **no** form to remove an ACL binding.

SYNTAX

ip arp inspection filter *arp-acl-name* **vlan** {*vlan-id* | *vlan-range*} [**static**]

arp-acl-name - Name of an ARP ACL. (Maximum length: 16 characters)

vlan-id - VLAN ID. (Range: 1-4094)

vlan-range - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

static - ARP packets are only validated against the specified ACL, address bindings in the DHCP snooping database is not checked.

DEFAULT SETTING

ARP ACLs are not bound to any VLAN
Static mode is not enabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- ARP ACLs are configured with the commands described on page 677.
- If static mode is enabled, the switch compares ARP packets to the specified ARP ACLs. Packets matching an IP-to-MAC address binding in a permit or deny rule are processed accordingly. Packets not matching any of the ACL rules are dropped. Address bindings in the DHCP snooping database are not checked.
- If static mode is not enabled, packets are first validated against the specified ARP ACL. Packets matching a deny rule are dropped. All remaining packets are validated against the address bindings in the DHCP snooping database.

EXAMPLE

```
Console(config)#ip arp inspection filter sales vlan 1
Console(config)#
```

ip arp inspection log-buffer logs

This command sets the maximum number of entries saved in a log message, and the rate at which these messages are sent. Use the **no** form to restore the default settings.

SYNTAX

ip arp inspection log-buffer logs *message-number* **interval** *seconds*

no ip arp inspection log-buffer logs

message-number - The maximum number of entries saved in a log message. (Range: 0-256, where 0 means no events are saved)

seconds - The interval at which log messages are sent. (Range: 0-86400)

DEFAULT SETTING

Message Number: 5
Interval: 1 second

COMMAND MODE

Global Configuration

COMMAND USAGE

- ARP Inspection must be enabled with the ip arp inspection command before this command will be accepted by the switch.
- By default, logging is active for ARP Inspection, and cannot be disabled.
- When the switch drops a packet, it places an entry in the log buffer. Each entry contains flow information, such as the receiving VLAN, the port number, the source and destination IP addresses, and the source and destination MAC addresses.
- If multiple, identical invalid ARP packets are received consecutively on the same VLAN, then the logging facility will only generate one entry in the log buffer and one corresponding system message.
- The maximum number of entries that can be stored in the log buffer is determined by the *message-number* parameter. If the log buffer fills up before a message is sent, the oldest entry will be replaced with the newest one.
- The switch generates a system message on a rate-controlled basis determined by the *seconds* values. After the system message is generated, all entries are cleared from the log buffer.

EXAMPLE

```
Console(config)#ip arp inspection log-buffer logs 1 interval 10
Console(config)#
```

ip arp inspection validate

This command specifies additional validation of address components in an ARP packet. Use the **no** form to restore the default setting.

SYNTAX

ip arp inspection validate {**dst-mac** [**ip**] [**src-mac**] | **ip** [**src-mac**] | **src-mac**}

no ip arp inspection validate

dst-mac - Checks the destination MAC address in the Ethernet header against the target MAC address in the ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

ip - Checks the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, while target IP addresses are checked only in ARP responses.

src-mac - Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

DEFAULT SETTING

No additional validation is performed

COMMAND MODE

Global Configuration

COMMAND USAGE

By default, ARP Inspection only checks the IP-to-MAC address bindings specified in an ARP ACL or in the DHCP Snooping database.

EXAMPLE

```
Console(config)#ip arp inspection validate dst-mac
Console(config)#
```

ip arp inspection vlan

This command enables ARP Inspection for a specified VLAN or range of VLANs. Use the **no** form to disable this function.

SYNTAX

[**no**] **ip arp inspection vlan** {*vlan-id* | *vlan-range*}

vlan-id - VLAN ID. (Range: 1-4094)

vlan-range - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

DEFAULT SETTING
Disabled on all VLANs

COMMAND MODE
Global Configuration

COMMAND USAGE
- When ARP Inspection is enabled globally with the ip arp inspection command, it becomes active only on those VLANs where it has been enabled with this command.
- When ARP Inspection is enabled globally and enabled on selected VLANs, all ARP request and reply packets on those VLANs are redirected to the CPU and their switching is handled by the ARP Inspection engine.
- When ARP Inspection is disabled globally, it becomes inactive for all VLANs, including those where ARP Inspection is enabled.
- When ARP Inspection is disabled, all ARP request and reply packets bypass the ARP Inspection engine and their manner of switching matches that of all other packets.
- Disabling and then re-enabling global ARP Inspection will not affect the ARP Inspection configuration for any VLANs.
- When ARP Inspection is disabled globally, it is still possible to configure ARP Inspection for individual VLANs. These configuration changes will only become active after ARP Inspection is globally enabled again.

EXAMPLE
```
Console(config)#ip arp inspection vlan 1,2
Console(config)#
```

ip arp inspection limit
This command sets a rate limit for the ARP packets received on a port. Use the **no** form to restore the default setting.

SYNTAX
ip arp inspection limit {**rate** *pps* | **none**}

no ip arp inspection limit

pps - The maximum number of ARP packets that can be processed by the CPU per second. (Range: 0-2048, where 0 means that no ARP packets can be forwarded)

none - There is no limit on the number of ARP packets that can be processed by the CPU.

DEFAULT SETTING
15

COMMAND MODE
Interface Configuration (Port)

COMMAND USAGE
- This command only applies to untrusted ports.
- When the rate of incoming ARP packets exceeds the configured limit, the switch drops all ARP packets in excess of the limit.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip arp inspection limit 150
Console(config-if)#
```

ip arp inspection trust

This command sets a port as trusted, and thus exempted from ARP Inspection. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **ip arp inspection trust**

DEFAULT SETTING
Untrusted

COMMAND MODE
Interface Configuration (Port)

COMMAND USAGE
Packets arriving on untrusted ports are subject to any configured ARP Inspection and additional validation checks. Packets arriving on trusted ports bypass all of these checks, and are forwarded according to normal switching rules.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip arp inspection trust
Console(config-if)#
```

show ip arp inspection configuration

This command displays the global configuration settings for ARP Inspection.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip arp inspection configuration

ARP inspection global information:

Global IP ARP Inspection status : disabled
Log Message Interval            : 10 s
Log Message Number              : 1
Need Additional Validation(s)   : Yes
Additional Validation Type      : Destination MAC address
Console#
```

show ip arp inspection interface

This command shows the trust status and ARP Inspection rate limit for ports.

SYNTAX

show ip arp inspection interface [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip arp inspection interface ethernet 1/1

Port Number        Trust Status             Limit Rate (pps)
-------------   --------------------    ------------------------------
Eth 1/1            trusted                    150
Console#
```

show ip arp inspection log

This command shows information about entries stored in the log, including the associated VLAN, port, and address components.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip arp inspection log
Total log entries number is 1

Num VLAN Port Src IP Address  Dst IP Address  Src MAC Address  Dst MAC Address
--- ---- ---- --------------  --------------  ---------------  --------------
1   1     11  192.168.2.2     192.168.2.1     00-04-E2-A0-E2-7C FF-FF-FF-FF-FF-FF
Console#
```

show ip arp inspection statistics

This command shows statistics about the number of ARP packets processed, or dropped for various reasons.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip arp inspection statistics

ARP packets received before rate limit                              : 150
ARP packets dropped due to rate limt                                : 5
Total ARP packets processed by ARP Inspection                       : 150
ARP packets dropped by additional validation (source MAC address)     : 0
ARP packets dropped by additional validation (destination MAC address): 0
ARP packets dropped by additional validation (IP address)           : 0
ARP packets dropped by ARP ACLs                                     : 0
ARP packets dropped by DHCP snooping                                : 0

Console#
```

show ip arp inspection vlan

This command shows the configuration settings for VLANs, including ARP Inspection status, the ARP ACL name, and if the DHCP Snooping database is used after ARP ACL validation is completed.

SYNTAX

show ip arp inspection vlan [*vlan-id* | *vlan-range*]

vlan-id - VLAN ID. (Range: 1-4094)

vlan-range - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip arp inspection vlan 1

VLAN ID     DAI Status             ACL Name             ACL Status
--------   ---------------    --------------------    --------------------
1           disabled               sales               static
Console#
```

26 ACCESS CONTROL LISTS

Access Control Lists (ACL) provide packet filtering for IPv4 frames (based on address, protocol, Layer 4 protocol port number or TCP control code), IPv6 frames (based on address or DSCP traffic class), or any frames (based on MAC address or Ethernet type). To filter packets, first create an access list, add the required rules, and then bind the list to a specific port. This section describes the Access Control List commands.

Table 84: Access Control List Commands

Command Group	Function
IPv4 ACLs	Configures ACLs based on IPv4 addresses, TCP/UDP port number, protocol type, and TCP control code
IPv6 ACLs	Configures ACLs based on IPv6 addresses or DSCP traffic class
MAC ACLs	Configures ACLs based on hardware addresses, packet format, and Ethernet type
ARP ACLs	Configures ACLs based on ARP messages addresses
ACL Information	Displays ACLs and associated rules; shows ACLs assigned to each port

IPv4 ACLs

The commands in this section configure ACLs based on IPv4 addresses, TCP/UDP port number, protocol type, and TCP control code. To configure IPv4 ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports.

Table 85: IPv4 ACL Commands

Command	Function	Mode
access-list ip	Creates an IP ACL and enters configuration mode for standard or extended IPv4 ACLs	GC
access-list rule-mode	Permits only extended rules, or permits both standard and extended rules	GC
permit, deny	Filters packets matching a specified source IPv4 address	IPv4-STD-ACL
permit, deny	Filters packets meeting the specified criteria, including source and destination IPv4 address, TCP/UDP port number, protocol type, and TCP control code	IPv4-EXT-ACL
ip access-group	Binds an IPv4 ACL to a port	IC
show ip access-group	Shows port assignments for IPv4 ACLs	PE
show ip access-list	Displays the rules for configured IPv4 ACLs	PE

access-list ip

This command adds an IP access list and enters configuration mode for standard or extended IPv4 ACLs. Use the **no** form to remove the specified ACL.

SYNTAX

[**no**] **access-list ip** {**standard** | **extended**} *acl-name*

standard – Specifies an ACL that filters packets based on the source IP address.

extended – Specifies an ACL that filters packets based on the source or destination IP address, and other more specific criteria.

acl-name – Name of the ACL. (Maximum length: 16 characters, no spaces or other special characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 100 rules.

EXAMPLE

```
Console(config)#access-list ip standard david
Console(config-std-acl)#
```

RELATED COMMANDS

permit, deny (662)
ip access-group (665)
show ip access-list (666)

access-list rule-mode

This command restricts access lists to only extended rules, or permits both standard and extended rules. Use the **no** form to restore the default setting.

SYNTAX

access-list rule-mode {**extended | mixed**}

no access-list rule-mode

extended – The system only permits extended rules, each of which occupies the space of two standard rules.

mixed – The system permits both standard and extended rules.

DEFAULT SETTING

Extended mode

COMMAND MODE

Global Configuration

COMMAND USAGE

When the rule mode is set to mixed, the following features are not supported:

- When the rule mode is changed, the change must be saved in the startup configuration file, and the switch rebooted for the new mode to take effect.
- When using extended rule mode, each rule used in an ACL occupies the space of two standard rules.
- When using mixed rule mode, either standard or extended rules can be used. However, the rules used in the same ACL must either be all standard or all extended rules. If standard rules are used for all ACLs, the maximum number of rules permitted by the system can be used.
- When using mixed rule mode, the following functions are not supported: DHCP Snooping, IP Source Guard, Web Authentication, Switch Cluster, UPnP, MAC-Based VLANs, and MVR.
- If the rule mode is changed from the default setting, the current status can be displayed with the show running-config and show startup-config commands.

EXAMPLE

```
Console(config)#access-list rule-mode extended
Warning: This will take effect only after rebooting the switch.
Console(config)#
```

permit, deny (Standard IP ACL)

This command adds a rule to a Standard IPv4 ACL. The rule sets a filter condition for packets emanating from the specified source. Use the **no** form to remove a rule.

SYNTAX

{**permit** | **deny**} {**any** | *source bitmask* | **host** *source*}
[**time-range** *time-range-name*]

no {**permit** | **deny**} {**any** | *source bitmask* | **host** *source*}

any – Any source IP address.

source – Source IP address.

bitmask – Decimal number representing the address bits to match.

host – Keyword followed by a specific IP address.

time-range-name - Name of the time range.
(Range: 1-30 characters)

DEFAULT SETTING

None

COMMAND MODE

Standard IPv4 ACL

COMMAND USAGE

- New rules are appended to the end of the list.
- Address bit masks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate "match" and 0 bits to indicate "ignore." The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

EXAMPLE

This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

```
Console(config-std-acl)#permit host 10.1.1.21
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

RELATED COMMANDS

access-list ip (660)
Time Range (515)

permit, deny (Extended IPv4 ACL)

This command adds a rule to an Extended IPv4 ACL. The rule sets a filter condition for packets with specific source or destination IP addresses, protocol types, source or destination protocol ports, or TCP control codes. Use the **no** form to remove a rule.

SYNTAX

{**permit** | **deny**} [*protocol-number* | **udp**]
{**any** | *source address-bitmask* | **host** *source*}
{**any** | *destination address-bitmask* | **host** *destination*}
[**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*]
[**source-port** *sport* [*bitmask*]]
[**destination-port** *dport* [*port-bitmask*]]
[**time-range** *time-range-name*]

no {**permit** | **deny**} [*protocol-number* | **udp**]
{**any** | *source address-bitmask* | **host** *source*}
{**any** | *destination address-bitmask* | **host** *destination*}
[**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*]
[**source-port** *sport* [*bitmask*]]
[**destination-port** *dport* [*port-bitmask*]]

{**permit** | **deny**} **tcp**
{**any** | *source address-bitmask* | **host** *source*}
{**any** | *destination address-bitmask* | **host** *destination*}
[**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*]
[**source-port** *sport* [*bitmask*]]
[**destination-port** *dport* [*port-bitmask*]]
[**control-flag** *control-flags flag-bitmask*]
[**time-range** *time-range-name*]

no {**permit** | **deny**} **tcp**
{**any** | *source address-bitmask* | **host** *source*}
{**any** | *destination address-bitmask* | **host** *destination*}
[**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*]
[**source-port** *sport* [*bitmask*]]
[**destination-port** *dport* [*port-bitmask*]]
[**control-flag** *control-flags flag-bitmask*]

protocol-number – A specific protocol number. (Range: 0-255)

source – Source IP address.

destination – Destination IP address.

address-bitmask – Decimal number representing the address bits to match.

host – Keyword followed by a specific IP address.

precedence – IP precedence level. (Range: 0-7)

tos – Type of Service level. (Range: 0-15)

dscp – DSCP priority level. (Range: 0-63)

sport – Protocol[17] source port number. (Range: 0-65535)

dport – Protocol[17] destination port number. (Range: 0-65535)

17. Includes TCP, UDP or other protocol types.

port-bitmask – Decimal number representing the port bits to match. (Range: 0-65535)

control-flags – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)

flag-bitmask – Decimal number representing the code bits to match.

time-range-name - Name of the time range. (Range: 1-30 characters)

DEFAULT SETTING
None

COMMAND MODE
Extended IPv4 ACL

COMMAND USAGE
- All new rules are appended to the end of the list.
- Address bit masks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate "match" and 0 bits to indicate "ignore." The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.
- You can specify both Precedence and ToS in the same rule. However, if DSCP is used, then neither Precedence nor ToS can be specified.
- The control-code bitmask is a decimal number (representing an equivalent bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit "1" means to match a bit and "0" means to ignore a bit. The following bits may be specified:
  - 1 (fin) – Finish
  - 2 (syn) – Synchronize
  - 4 (rst) – Reset
  - 8 (psh) – Push
  - 16 (ack) – Acknowledgement
  - 32 (urg) – Urgent pointer

  For example, use the code value and mask below to catch packets with the following flags set:
  - SYN flag valid, use "control-code 2 2"
  - Both SYN and ACK valid, use "control-code 18 18"
  - SYN valid and ACK invalid, use "control-code 2 18"

EXAMPLE

This example accepts any incoming packets if the source address is within subnet 10.7.1.x. For example, if the rule is matched; i.e., the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any
Console(config-ext-acl)#
```

This allows TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (i.e., HTTP).

```
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any destination-port
  80
Console(config-ext-acl)#
```

This permits all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to "SYN."

```
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any control-
  flag 2 2
Console(config-ext-acl)#
```

RELATED COMMANDS

access-list ip (660)
Time Range (515)

ip access-group

This command binds an IPv4 ACL to a port. Use the **no** form to remove the port.

SYNTAX

ip access-group *acl-name* **in** [**time-range** *time-range-name*]

no ip access-group *acl-name* **in**

acl-name – Name of the ACL. (Maximum length: 16 characters)

in – Indicates that this list applies to ingress packets.

time-range-name - Name of the time range.
(Range: 1-30 characters)

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- Only one ACL can be bound to a port.
- If an ACL is already bound to a port and you bind a different ACL to it, the switch will replace the old binding with the new one.

EXAMPLE

```
Console(config)#int eth 1/2
Console(config-if)#ip access-group david in
Console(config-if)#
```

RELATED COMMANDS

show ip access-list (666)
Time Range (515)

show ip access-group

This command shows the ports assigned to IP ACLs.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip access-group
Interface ethernet 1/2
 IP access-list david in
Console#
```

RELATED COMMANDS

ip access-group (665)

show ip access-list

This command displays the rules for configured IPv4 ACLs.

SYNTAX

show ip access-list {**standard** | **extended**} [*acl-name*]

standard – Specifies a standard IP ACL.

extended – Specifies an extended IP ACL.

acl-name – Name of the ACL. (Maximum length: 16 characters)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip access-list standard
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 255.255.15.0
Console#
```

RELATED COMMANDS

permit, deny (662)
ip access-group (665)

IPv6 ACLs

The commands in this section configure ACLs based on IPv6 addresses, next header type, and flow label. To configure IPv6 ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports.

Table 86: IPv4 ACL Commands

Command	Function	Mode
access-list ipv6	Creates an IPv6 ACL and enters configuration mode for standard or extended IPv6 ACLs	GC
permit, deny	Filters packets matching a specified source IPv6 address	IPv6-STD-ACL
permit, deny	Filters packets meeting the specified criteria, including destination IPv6 address, next header type, and flow label	IPv6-EXT-ACL
show ipv6 access-list	Displays the rules for configured IPv6 ACLs	PE
ipv6 access-group	Adds a port to an IPv6 ACL	IC
show ipv6 access-group	Shows port assignments for IPv6 ACLs	PE

access-list ipv6

This command adds an IP access list and enters configuration mode for standard or extended IPv6 ACLs. Use the **no** form to remove the specified ACL.

SYNTAX

[**no**] **access-list ipv6** {**standard** | **extended**} *acl-name*

standard – Specifies an ACL that filters packets based on the source IP address.

extended – Specifies an ACL that filters packets based on the destination IP address, and other more specific criteria.

acl-name – Name of the ACL. (Maximum length: 16 characters)

DEFAULT SETTING

None

COMMAND MODE
Global Configuration

COMMAND USAGE
- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 64 rules.

EXAMPLE
```
Console(config)#access-list ipv6 standard david
Console(config-std-ipv6-acl)#
```

RELATED COMMANDS
permit, deny (Standard IPv6 ACL) (668)
permit, deny (Extended IPv6 ACL) (669)
ipv6 access-group (671)
show ipv6 access-list (670)

permit, deny (Standard IPv6 ACL)

This command adds a rule to a Standard IPv6 ACL. The rule sets a filter condition for packets emanating from the specified source. Use the **no** form to remove a rule.

SYNTAX
{**permit** | **deny**} {**any** | **host** *source-ipv6-address* | *source-ipv6-address*[*/prefix-length*]} [**time-range** *time-range-name*]

no {**permit** | **deny**} {**any** | **host** *source-ipv6-address* | *source-ipv6-address*[*/prefix-length*]}

any – Any source IP address.

host – Keyword followed by a specific IP address.

source-ipv6-address - An IPv6 source address or network class. The address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix; i.e., the network portion of the address. (Range: 0-128)

time-range-name - Name of the time range. (Range: 1-30 characters)

DEFAULT SETTING
None

COMMAND MODE
Standard IPv6 ACL

COMMAND USAGE
New rules are appended to the end of the list.

EXAMPLE
This example configures one permit rule for the specific address 2009:DB9:2229::79 and another rule for the addresses with the network prefix 2009:DB9:2229:5::/64.

```
Console(config-std-ipv6-acl)#permit host 2009:DB9:2229::79
Console(config-std-ipv6-acl)#permit 2009:DB9:2229:5::/64
Console(config-std-ipv6-acl)#
```

RELATED COMMANDS
access-list ipv6 (667)
Time Range (515)

permit, deny (Extended IPv6 ACL)

This command adds a rule to an Extended IPv6 ACL. The rule sets a filter condition for packets with specific destination IP addresses, next header type, or flow label. Use the **no** form to remove a rule.

SYNTAX

{**permit** | **deny**} {**any** | **host** *source-ipv6-address* | *source-ipv6-address*[*/prefix-length*]} {**any** | *destination-ipv6-address*[*/prefix-length*]} [**dscp** *dscp*] [**time-range** *time-range-name*]

no {**permit** | **deny**} {**any** | **host** *source-ipv6-address* | *source-ipv6-address*[*/prefix-length*]} {**any** | *destination-ipv6-address*[*/prefix-length*]} [**dscp** *dscp*]

any – Any IP address (an abbreviation for the IPv6 prefix ::/0).

host – Keyword followed by a specific source IP address.

source-ipv6-address - An IPv6 source address or network class. The address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

destination-ipv6-address - An IPv6 destination address or network class. The address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the

undefined fields. (The switch only checks the first 64 bits of the destination address.)

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix; i.e., the network portion of the address. (Range: 0-128 for source prefix, 0-8 for destination prefix)

dscp – DSCP traffic class. (Range: 0-63)

time-range-name - Name of the time range. (Range: 1-30 characters)

DEFAULT SETTING
None

COMMAND MODE
Extended IPv6 ACL

COMMAND USAGE
All new rules are appended to the end of the list.

EXAMPLE
This example accepts any incoming packets if the destination address is 2009:DB9:2229::79/8.

```
Console(config-ext-ipv6-acl)#permit 2009:DB9:2229::79/8
Console(config-ext-ipv6-acl)#
```

This allows packets to any destination address when the DSCP value is 5.

```
Console(config-ext-ipv6-acl)#permit any dscp 5
Console(config-ext-ipv6-acl)#
```

RELATED COMMANDS
access-list ipv6 (667)
Time Range (515)

show ipv6 access-list

This command displays the rules for configured IPv6 ACLs.

SYNTAX
show ipv6 access-list {**standard** | **extended**} [*acl-name*]

standard – Specifies a standard IPv6 ACL.

extended – Specifies an extended IPv6 ACL.

acl-name – Name of the ACL. (Maximum length: 16 characters)

COMMAND MODE
Privileged Exec

EXAMPLE

```
Console#show ipv6 access-list standard
IPv6 standard access-list david:
  permit host 2009:DB9:2229::79
  permit 2009:DB9:2229:5::/64
Console#
```

RELATED COMMANDS

permit, deny (Standard IPv6 ACL) (668)
permit, deny (Extended IPv6 ACL) (669)
ipv6 access-group (671)

ipv6 access-group

This command binds a port to an IPv6 ACL. Use the **no** form to remove the port.

SYNTAX

ipv6 access-group *acl-name* **in** [**time-range** *time-range-name*]

no ipv6 access-group *acl-name* **in**

acl-name – Name of the ACL. (Maximum length: 16 characters)

in – Indicates that this list applies to ingress packets.

time-range-name - Name of the time range.
(Range: 1-30 characters)

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- A port can only be bound to one ACL.
- If a port is already bound to an ACL and you bind it to a different ACL, the switch will replace the old binding with the new one.
- IPv6 ACLs can only be applied to ingress packets.

EXAMPLE

```
Console(config)#int eth 1/2
Console(config-if)#ipv6 access-group standard david in
Console(config-if)#
```

RELATED COMMANDS

show ipv6 access-list (670)
Time Range (515)

show ipv6 access-group

This command shows the ports assigned to IPv6 ACLs.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip access-group
Interface ethernet 1/2
 IPv6 standard access-list david in
Console#
```

RELATED COMMANDS

ipv6 access-group (671)

MAC ACLs

The commands in this section configure ACLs based on hardware addresses, packet format, and Ethernet type. To configure MAC ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports.

Table 87: MAC ACL Commands

Command	Function	Mode
access-list mac	Creates a MAC ACL and enters configuration mode	GC
permit, deny	Filters packets matching a specified source and destination address, packet format, and Ethernet type	MAC-ACL
mac access-group	Binds a MAC ACL to a port	IC
show mac access-group	Shows port assignments for MAC ACLs	PE
show mac access-list	Displays the rules for configured MAC ACLs	PE

access-list mac

This command adds a MAC access list and enters MAC ACL configuration mode. Use the **no** form to remove the specified ACL.

SYNTAX

[**no**] **access-list mac** *acl-name*

acl-name – Name of the ACL. (Maximum length: 16 characters, no spaces or other special characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 64 rules.

EXAMPLE

```
Console(config)#access-list mac jerry
Console(config-mac-acl)#
```

RELATED COMMANDS

permit, deny (673)
mac access-group (675)
show mac access-list (676)

permit, deny (MAC ACL)

This command adds a rule to a MAC ACL. The rule filters packets matching a specified MAC source or destination address (i.e., physical layer address), or Ethernet protocol type. Use the **no** form to remove a rule.

SYNTAX

{**permit** | **deny**}
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**cos** *cos cos-bitmask*] [**vid** *vid vid-bitmask*]
[**ethertype** *protocol* [*protocol-bitmask*]]
[**time-range** *time-range-name*]

no {**permit** | **deny**}
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**cos** *cos cos-bitmask*] [**vid** *vid vid-bitmask*]
[**ethertype** *protocol* [*protocol-bitmask*]]

NOTE: The default is for Ethernet II packets.

{**permit** | **deny**} **tagged-eth2**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**cos** *cos cos-bitmask*] [**vid** *vid vid-bitmask*]
[**ethertype** *protocol* [*protocol-bitmask*]]
[**time-range** *time-range-name*]

no {**permit** | **deny**} **tagged-eth2**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**cos** *cos cos-bitmask*] [**vid** *vid vid-bitmask*]
[**ethertype** *protocol* [*protocol-bitmask*]]

{**permit** | **deny**} **untagged-eth2**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**ethertype** *protocol* [*protocol-bitmask*]]
[**time-range** *time-range-name*]

no {**permit** | **deny**} **untagged-eth2**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**ethertype** *protocol* [*protocol-bitmask*]]

{**permit** | **deny**} **tagged-802.3**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**cos** *cos cos-bitmask*] [**vid** *vid vid-bitmask*]
[**time-range** *time-range-name*]

no {**permit** | **deny**} **tagged-802.3**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**cos** *cos cos-bitmask*] [**vid** *vid vid-bitmask*]

{**permit** | **deny**} **untagged-802.3**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**time-range** *time-range-name*]

no {**permit** | **deny**} **untagged-802.3**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}

tagged-eth2 – Tagged Ethernet II packets.

untagged-eth2 – Untagged Ethernet II packets.

tagged-802.3 – Tagged Ethernet 802.3 packets.

untagged-802.3 – Untagged Ethernet 802.3 packets.

any – Any MAC source or destination address.

host – A specific MAC address.

source – Source MAC address.

destination – Destination MAC address range with bitmask.

address-bitmask[18] – Bitmask for MAC address (in hexadecimal format).

cos – Class-of-Service value (Range: 0-7)

cos-bitmask[18] – Class-of-Service bitmask. (Range: 0-7)

vid – VLAN ID. (Range: 1-4094)

18. For all bitmasks, “1” means care and “0” means ignore.

vid-bitmask[18] – VLAN bitmask. (Range: 0-4095)

protocol – A specific Ethernet protocol number. (Range: 600-ffff hex.)

protocol-bitmask[18] – Protocol bitmask. (Range: 600-ffff hex.)

time-range-name - Name of the time range. (Range: 1-30 characters)

DEFAULT SETTING
None

COMMAND MODE
MAC ACL

COMMAND USAGE
- New rules are added to the end of the list.
- The **ethertype** option can only be used to filter Ethernet II formatted packets.
- A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include the following:
  - 0800 - IP
  - 0806 - ARP
  - 8137 - IPX

EXAMPLE
This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de ethertype 0800
Console(config-mac-acl)#
```

RELATED COMMANDS
access-list mac (672)
Time Range (515)

mac access-group

This command binds a MAC ACL to a port. Use the **no** form to remove the port.

SYNTAX
mac access-group *acl-name* **in** [**time-range** *time-range-name*]

acl-name – Name of the ACL. (Maximum length: 16 characters)

in – Indicates that this list applies to ingress packets.

time-range-name - Name of the time range. (Range: 1-30 characters)

DEFAULT SETTING
None

COMMAND MODE
Interface Configuration (Ethernet)

COMMAND USAGE
- Only one ACL can be bound to a port.
- If an ACL is already bound to a port and you bind a different ACL to it, the switch will replace the old binding with the new one.

EXAMPLE
```
Console(config)#interface ethernet 1/2
Console(config-if)#mac access-group jerry in
Console(config-if)#
```

RELATED COMMANDS
show mac access-list (676)
Time Range (515)

show mac access-group
This command shows the ports assigned to MAC ACLs.

COMMAND MODE
Privileged Exec

EXAMPLE
```
Console#show mac access-group
Interface ethernet 1/5
 MAC access-list M5 in
Console#
```

RELATED COMMANDS
mac access-group (675)

show mac access-list
This command displays the rules for configured MAC ACLs.

SYNTAX
show mac access-list [*acl-name*]

acl-name – Name of the ACL. (Maximum length: 16 characters)

COMMAND MODE
Privileged Exec

EXAMPLE

```
Console#show mac access-list
MAC access-list jerry:
  permit any 00-e0-29-94-34-de ethertype 0800
Console#
```

RELATED COMMANDS

permit, deny (673)
mac access-group (675)

ARP ACLs

The commands in this section configure ACLs based on the IP or MAC address contained in ARP request and reply messages. To configure ARP ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more VLANs using the ip arp inspection vlan command.

Table 88: ARP ACL Commands

Command	Function	Mode
access-list arp	Creates a ARP ACL and enters configuration mode	GC
permit, deny	Filters packets matching a specified source or destination address in ARP messages	ARP-ACL
show arp access-list	Displays the rules for configured ARP ACLs	PE

access-list arp

This command adds an ARP access list and enters ARP ACL configuration mode. Use the **no** form to remove the specified ACL.

SYNTAX

[**no**] **access-list arp** *acl-name*

acl-name – Name of the ACL. (Maximum length: 16 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.

- An ACL can contain up to 64 rules.

EXAMPLE

```
Console(config)#access-list arp factory
Console(config-arp-acl)#
```

RELATED COMMANDS

permit, deny (678)
show arp access-list (679)

permit, deny (ARP ACL)

This command adds a rule to an ARP ACL. The rule filters packets matching a specified source or destination address in ARP messages. Use the **no** form to remove a rule.

SYNTAX

[**no**] {**permit** | **deny**}
ip {**any** | **host** *source-ip* | *source-ip ip-address-bitmask*}
mac {**any** | **host** *source-ip* | *source-ip ip-address-bitmask*} [**log**]

This form indicates either request or response packets.

[**no**] {**permit** | **deny**} **request**
ip {**any** | **host** *source-ip* | *source-ip ip-address-bitmask*}
mac {**any** | **host** *source-mac* | *source-mac mac-address-bitmask*} [**log**]

[**no**] {**permit** | **deny**} **response**
ip {**any** | **host** *source-ip* | *source-ip ip-address-bitmask*} {**any** | **host** *destination-ip* | *destination-ip ip-address-bitmask*}
mac {**any** | **host** *source-mac* | *source-mac mac-address-bitmask*} [**any** | **host** *destination-mac* | *destination-mac mac-address-bitmask*] [**log**]

source-ip – Source IP address.

destination-ip – Destination IP address with bitmask.

ip-address-bitmask[19] – IPv4 number representing the address bits to match.

source-mac – Source MAC address.

destination-mac – Destination MAC address range with bitmask.

mac-address-bitmask[19] – Bitmask for MAC address (in hexadecimal format).

log - Logs a packet when it matches the access control entry.

DEFAULT SETTING

None

19. For all bitmasks, binary "1" means care and "0" means ignore.

COMMAND MODE
ARP ACL

COMMAND USAGE
New rules are added to the end of the list.

EXAMPLE
This rule permits packets from any source IP and MAC address to the destination subnet address 192.168.0.0.

```
Console(config-arp-acl)#$permit response ip any 192.168.0.0 255.255.0.0 mac
  any any
Console(config-mac-acl)#
```

RELATED COMMANDS
access-list arp (677)

show arp access-list
This command displays the rules for configured ARP ACLs.

SYNTAX
show arp access-list [*acl-name*]

acl-name – Name of the ACL. (Maximum length: 16 characters)

COMMAND MODE
Privileged Exec

EXAMPLE

```
Console#show arp access-list
ARP access-list factory:
  permit response ip any 192.168.0.0 255.255.0.0 mac any any
Console#
```

RELATED COMMANDS
permit, deny (678)

ACL INFORMATION

This section describes commands used to display ACL information.

Table 89: ACL Information Commands

Command	Function	Mode
show access-group	Shows the ACLs assigned to each port	PE
show access-list	Show all ACLs and associated rules	PE

show access-group

This command shows the port assignments of ACLs.

COMMAND MODE

Privileged Executive

EXAMPLE

```
Console#show access-group
Interface ethernet 1/2
 IP access-list david
 MAC access-list jerry
Console#
```

show access-list

This command shows all ACLs and associated rules.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show access-list
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 255.255.15.0
IP extended access-list bob:
  permit 10.7.1.1 255.255.255.0 any
  permit 192.168.1.0 255.255.255.0 any destination-port 80 80
  permit 192.168.1.0 255.255.255.0 any protocol tcp control-code 2 2
MAC access-list jerry:
  permit any host 00-30-29-94-34-de ethertype 800 800
IP extended access-list A6:
  deny tcp any any control-flag 2 2
  permit any any
Console#
```

27 INTERFACE COMMANDS

These commands are used to display or set communication parameters for an Ethernet port, aggregated link, or VLAN; or perform cable diagnostics on the specified interface.

Table 90: Interface Commands

Command	Function	Mode
interface	Configures an interface type and enters interface configuration mode	GC
capabilities	Advertises the capabilities of a given interface for use in autonegotiation	IC
description	Adds a description to an interface configuration	IC
flowcontrol	Enables flow control on a given interface	IC
giga-phy-mode	Forces two connected ports in to a master/slave configuration to enable 1000BASE-T full duplex	IC
mdix	Sets pinout configuration to automatic detection or fixed mode	IC
media-type	Force port type selected for combination ports	IC
negotiation	Enables autonegotiation of a given interface	IC
shutdown	Disables an interface	IC
speed-duplex	Configures the speed and duplex operation of a given interface when autonegotiation is disabled	IC
switchport packet-rate*	Configures broadcast, multicast, and unknown unicast storm control thresholds	IC
clear counters	Clears statistics on an interface	PE
show interfaces brief	Displays a summary of key information, including operational status, native VLAN ID, default priority, speed/duplex mode, and port type	PE
show interfaces counters	Displays statistics for the specified interfaces	NE, PE
show interfaces status	Displays status for the specified interface	NE, PE
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE
show interfaces transceiver	Displays the temperature, voltage, bias current, transmit power, and receive power	PE
Cable Diagnostics		
test cable-diagnostics tdr interface	Performs cable diagnostics on the specified port	PE
show cable-diagnostics	Shows the results of a cable diagnostics test	PE

* Enabling hardware-level storm control with this command on a port will disable software-level automatic storm control on the same port if configured by the auto-traffic-control command.

interface

This command configures an interface type and enter interface configuration mode. Use the **no** form with a trunk to remove an inactive interface.

SYNTAX

[**no**] **interface** *interface*

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

vlan *vlan-id* (Range: 1-4093)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

EXAMPLE

To specify port 4, enter the following command:

```
Console(config)#interface ethernet 1/4
Console(config-if)#
```

capabilities

This command advertises the port capabilities of a given interface during auto-negotiation. Use the **no** form with parameters to remove an advertised capability, or the **no** form without parameters to restore the default values.

SYNTAX

[**no**] **capabilities** {**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**}

1000full - Supports 1 Gbps full-duplex operation

100full - Supports 100 Mbps full-duplex operation

100half - Supports 100 Mbps half-duplex operation

10full - Supports 10 Mbps full-duplex operation

10half - Supports 10 Mbps half-duplex operation

flowcontrol - Supports flow control

symmetric (Gigabit only) - When specified, the port transmits and receives pause frames. *(The current switch ASIC only supports symmetric pause frames.)*

DEFAULT SETTING
100BASE-TX: 10half, 10full, 100half, 100full
1000BASE-T: 10half, 10full, 100half, 100full, 1000full
1000BASE-SX/LX/LH (SFP): 1000full

COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE
- The 1000BASE-T standard does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk.
- When auto-negotiation is enabled with the negotiation command, the switch will negotiate the best settings for a link based on the **capabilities** command. When auto-negotiation is disabled, you must manually specify the link attributes with the speed-duplex and flowcontrol commands.

EXAMPLE
The following example configures Ethernet port 5 capabilities to include 100half and 100full.

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

RELATED COMMANDS
negotiation (688)
speed-duplex (689)
flowcontrol (684)

description
This command adds a description to an interface. Use the **no** form to remove the description.

SYNTAX
description *string*

no description

string - Comment or a description to help you remember what is attached to this interface. (Range: 1-64 characters)

DEFAULT SETTING
None

COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

The description is displayed by the show interfaces status command and in the running-configuration file. An example of the value which a network manager might store in this object is the name of the manufacturer, and the product name.

EXAMPLE

The following example adds a description to port 4.

```
Console(config)#interface ethernet 1/4
Console(config-if)#description RD-SW#3
Console(config-if)#
```

flowcontrol

This command enables flow control. Use the **no** form to disable flow control.

SYNTAX

[**no**] **flowcontrol**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- 1000BASE-T does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk.
- Flow control can eliminate frame loss by "blocking" traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3-2002 (formally IEEE 802.3x) for full-duplex operation.
- To force flow control on or off (with the **flowcontrol** or **no flowcontrol** command), use the no negotiation command to disable auto-negotiation on the selected interface.
- When using the negotiation command to enable auto-negotiation, the optimal settings will be determined by the capabilities command. To enable flow control under auto-negotiation, "flowcontrol" must be included in the capabilities list for any port
- Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.

EXAMPLE

The following example enables flow control on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

RELATED COMMANDS

negotiation (688)
capabilities (flowcontrol, symmetric) (682)

giga-phy-mode

This command forces two connected ports into a master/slave configuration to enable 1000BASE-T full duplex for Gigabit ports 25-28 (ES3528M) and 49-52 (ES3552M). Use the **no** form to restore the default mode.

SYNTAX

giga-phy-mode *mode*

no giga-phy-mode

mode

master - Sets the selected port as master.

slave - Sets the selected port as slave.

auto-prefer-master - Uses master mode as the initial configuration setting regardless of the mode configured at the other end of the link.

auto-prefer-slave - Uses slave mode as the initial configuration regardless of the mode configured at the other end of the link.

DEFAULT SETTING

master

COMMAND MODE

Interface Configuration (Ethernet - Ports 25-28/49-52)

COMMAND USAGE

- The 1000BASE-T standard does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk. If not used, the success of the link process cannot be guaranteed when connecting to other types of switches. However, this switch does provide a means of forcing a link to operate at 1000 Mbps, full-duplex using the **giga-phy-mode** command.

- To force 1000full operation requires the ports at both ends of a link to establish their role in the connection process as a master or slave. Before using this feature, auto-negotiation must first be disabled, and

the Speed/Duplex attribute set to 1000full. Then select compatible Giga PHY modes at both ends of the link. Note that using one of the preferred modes ensures that the ports at both ends of a link will eventually cooperate to establish a valid master-slave relationship.

EXAMPLE

This forces the switch port to master mode on port 24.

```
Console(config)#interface ethernet 1/24
Console(config-if)#no negotiation
Console(config-if)#speed-duplex 1000full
Console(config-if)#giga-phy-mode master
Console(config-if)#
```

mdix

This command sets pinout configuration to automatic detection or fixed mode for MDI/MDI-X signaling on any of the RJ-45 ports. Use the no form to restore the default mode.

SYNTAX

mdix {**auto** | **crossover** | **straight**}

auto - Automatically detects the pinout configuration of the attached device, and negotiates with the link partner to determine which side will adjust the pinout signals if required to ensure a proper connection.

crossover - Specifies a fixed setting for MDI-X (i.e., crossover).

straight - Specifies a fixed setting for MDI (i.e., straight-through).

DEFAULT SETTING

auto

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

Auto-negotiation must be enabled to use the "auto" option for this command. It must be disabled to force the pinout setting to one of the fixed modes of "straight" (MDI) or "crossover" (MDI-X).

One side of a link must be configured with MDI pinouts and the other side with MDI-X pinouts to ensure that signals sent from the transmit pins on one side of the link are received on the receive pins by the link partner. For more information on the signals used for each of these pinout types, refer to the Installation Guide.

EXAMPLE

This example forces the Port 1 to MDI mode.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mdix straight
Console(config-if)#
```

RELATED COMMANDS

negotiation (688)

media-type

This command forces the port type selected for combination ports 25-28 (ES3528M) and 49-52 (ES3552M). Use the **no** form to restore the default mode.

SYNTAX

media-type *mode*

no media-type

mode

copper-forced - Always uses the built-in RJ-45 port.

sfp-forced - Always uses the SFP port (even if module not installed).

sfp-preferred-auto - Uses SFP port if both combination types are functioning and the SFP port has a valid link.

DEFAULT SETTING

sfp-preferred-auto

COMMAND MODE

Interface Configuration (Ethernet - Ports 25-28/49-52)

EXAMPLE

This forces the switch to use the built-in RJ-45 port for the combination port 25.

```
Console(config)#interface ethernet 1/25
Console(config-if)#media-type copper-forced
Console(config-if)#
```

negotiation

This command enables auto-negotiation for a given interface. Use the **no** form to disable auto-negotiation.

SYNTAX

[**no**] **negotiation**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- 1000BASE-T does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk.
- When auto-negotiation is enabled the switch will negotiate the best settings for a link based on the capabilities command. When auto-negotiation is disabled, you must manually specify the link attributes with the speed-duplex and flowcontrol commands.
- If auto-negotiation is disabled, auto-MDI/MDI-X pin signal configuration will also be disabled for the RJ-45 ports.

EXAMPLE

The following example configures port 10 to use auto-negotiation.

```
Console(config)#interface ethernet 1/10
Console(config-if)#negotiation
Console(config-if)#
```

RELATED COMMANDS

capabilities (682)
speed-duplex (689)

shutdown

This command disables an interface. To restart a disabled interface, use the **no** form.

SYNTAX

[**no**] **shutdown**

DEFAULT SETTING

All interfaces are enabled.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This command allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also want to disable a port for security reasons.

EXAMPLE

The following example disables port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#shutdown
Console(config-if)#
```

speed-duplex

This command configures the speed and duplex mode of a given interface when auto-negotiation is disabled. Use the **no** form to restore the default.

SYNTAX

speed-duplex {**100full** | **100half** | **10full** | **10half**}

no speed-duplex

100full - Forces 100 Mbps full-duplex operation

100half - Forces 100 Mbps half-duplex operation

10full - Forces 10 Mbps full-duplex operation

10half - Forces 10 Mbps half-duplex operation

DEFAULT SETTING

- Auto-negotiation is enabled by default.
- When auto-negotiation is disabled, the default speed-duplex setting is:
  - Fast Ethernet ports – **100full** for 100BASE-TX ports
  - Gigabit Ethernet ports – **100full** for 1000BASE-T ports

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- The 1000BASE-T standard does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk. If not used, the success of the link process cannot be guaranteed when connecting to other types of switches. However, this switch does provide a means of safely forcing a link to operate at 1000 Mbps, full-duplex using the giga-phy-mode command.
- To force operation to the speed and duplex mode specified in a **speed-duplex** command, use the no negotiation command to disable auto-negotiation on the selected interface.
- When using the negotiation command to enable auto-negotiation, the optimal settings will be determined by the capabilities command. To set

the speed/duplex mode under auto-negotiation, the required mode must be specified in the capabilities list for an interface.

EXAMPLE

The following example configures port 5 to 100 Mbps, half-duplex operation.

```
Console(config)#interface ethernet 1/5
Console(config-if)#speed-duplex 100half
Console(config-if)#no negotiation
Console(config-if)#
```

RELATED COMMANDS

negotiation (688)
capabilities (682)

switchport packet-rate

This command configures broadcast, multicast and unknown unicast storm control. Use the **no** form to restore the default setting.

SYNTAX

switchport {**broadcast** | **multicast** | **unicast**} **packet-rate** *rate*

no switchport {**broadcast** | **multicast** | **unicast**}

broadcast - Specifies storm control for broadcast traffic.

multicast - Specifies storm control for multicast traffic.

unicast - Specifies storm control for unknown unicast traffic.

rate - Threshold level as a rate; i.e., kilobits per second.
(Range: 64-100000 Kbps for Fast Ethernet ports,
64-1000000 Kbps for Gigabit Ethernet ports)

DEFAULT SETTING

Broadcast Storm Control: Enabled, packet-rate limit: 64 kbps
Multicast Storm Control: Disabled
Unknown Unicast Storm Control: Disabled

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- When traffic exceeds the threshold specified for broadcast and multicast or unknown unicast traffic, packets exceeding the threshold are dropped until the rate falls back down beneath the threshold.
- Due to an ASIC chip limitation, the supported storm control modes include:
  - broadcast
  - broadcast + multicast
  - broadcast + multicast + unknown unicast

This means that when multicast storm control is enabled, broadcast storm control is also enabled (using the threshold value set by the multicast storm control command). And when unknown unicast storm control is enabled, broadcast and multicast storm control are also enabled (using the threshold value set by the unknown unicast storm control command).

- Traffic storms can be controlled at the hardware level using this command or at the software level using the auto-traffic-control command. However, only one of these control types can be applied to a port. Enabling hardware-level storm control on a port will disable automatic storm control on that port.
- The rate limits set by this command are also used by automatic storm control when the control response is set to rate limiting by the auto-traffic-control action command.
- Using both rate limiting and storm control on the same interface may lead to unexpected results. For example, suppose broadcast storm control is set to 500 Kbps by the command "switchport broadcast packet-rate 500," and the rate limit is set to 20000 Kbps by the command "rate-limit input 20000" on a Fast Ethernet port. Since 20000 Kbps is 1/5 of line speed (100 Mbps), the received rate will actually be 100 Kbps, or 1/5 of the 500 Kbps limit set by the storm control command. It is therefore not advisable to use both of these commands on the same interface.

EXAMPLE

The following shows how to configure broadcast storm control at 600 kilobits per second:

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast packet-rate 600
Console(config-if)#
```

clear counters

This command clears statistics on an interface.

SYNTAX

clear counters *interface*

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

None

COMMAND MODE
Privileged Exec

COMMAND USAGE
Statistics are only initialized for a power reset. This command sets the base value for displayed statistics to zero for the current management session. However, if you log out and back into the management interface, the statistics displayed will show the absolute value accumulated since the last power reset.

EXAMPLE
The following example clears statistics on port 5.

```
Console#clear counters ethernet 1/5
Console#
```

show interfaces brief

This command displays a summary of key information, including operational status, native VLAN ID, default priority, speed/duplex mode, and port type for all ports.

COMMAND MODE
Privileged Exec

EXAMPLE

```
Console#show interfaces brief
Interface Name               Status   PVID Pri Speed/Duplex  Type         Trunk
--------- ------------------ -------- ---- --- ------------- ------------ ---
Eth 1/ 1                     Up          1   0 Auto-100full  100TX        None
Eth 1/ 2                     Down        1   0 Auto          100TX        None
Eth 1/ 3                     Down        1   0 Auto          100TX        None
Eth 1/ 4                     Down        1   0 Auto          100TX        None
Eth 1/ 5                     Down        1   0 Auto          100TX        None
Eth 1/ 6                     Down        1   0 Auto          100TX        None
:
```

show interfaces counters

This command displays interface statistics.

SYNTAX

show interfaces counters [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING
Shows the counters for all interfaces.

COMMAND MODE
Normal Exec, Privileged Exec

COMMAND USAGE
If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see "Showing Port or Trunk Statistics."

EXAMPLE

```
Console#show interfaces counters ethernet 1/1
Ethernet 1/ 1
 Iftable Stats:
  Octets Input: 227660, Octets Output: 1403234
  Unicast Input: 1236, Unicast Output: 1387
  Discard Input: 0, Discard Output: 0
  Error Input: 0, Error Output: 0
  Unknown Protos Input: 0, QLen Output: 0
 Extended Iftable Stats:
  Multi-cast Input: 862, Multi-cast Output: 918
  Broadcast Input: 26, Broadcast Output: 3
 Ether-like Stats:
  Alignment Errors: 0, FCS Errors: 0
  Single Collision Frames: 0, Multiple Collision Frames: 0
  SQE Test Errors: 0, Deferred Transmissions: 0
  Late Collisions: 0, Excessive Collisions: 0
  Internal Mac Transmit Errors: 0, Internal Mac Receive Errors: 0
  Frames Too Long: 0, Carrier Sense Errors: 0
  Symbol Errors: 0
 RMON Stats:
  Drop Events: 0, Octets: 1631150, Packets: 4434
  Broadcast PKTS: 29, Multi-cast PKTS: 1782
  Undersize PKTS: 0, Oversize PKTS: 0
  Fragments: 0, Jabbers: 0
  CRC Align Errors: 0, Collisions: 0
  Packet Size <= 64 Octets: 3049, Packet Size 65 to 127 Octets: 163
  Packet Size 128 to 255 Octets: 141, Packet Size 256 to 511 Octets: 11
  Packet Size 512 to 1023 Octets: 272, Packet Size 1024 to 1518 Octets: 798
 Port Utilization (recent 300 seconds):
  Input Rate  : 0 kbits/sec, 1 Pkts/sec,   0.00% Utilization
  Output Rate : 5 kbits/sec, 1 Pkts/sec,   0.00% Utilization
Console#
```

show interfaces status

This command displays the status for an interface.

SYNTAX

show interfaces status [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

vlan *vlan-id* (Range: 1-4093)

DEFAULT SETTING

Shows the status for all interfaces.

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see "Displaying Connection Status."

EXAMPLE

```
Console#show interfaces status ethernet 1/25
 Basic Information:
  Port Type:              1000T
  Mac Address:            00-12-CF-61-24-48
 Configuration:
  Name:
  Port Admin:             Up
  MDIX mode:              Auto
  Speed-duplex:           Auto
  Capabilities:           10half, 10full, 100half, 100full, 1000full
  Broadcast Storm:        Enabled
  Broadcast Storm Limit:  64 Kbits/second
  Multicast Storm:        Disabled
  Multicast Storm Limit:  64 Kbits/second
  UnknownUnicast Storm:       Disabled
  UnknownUnicast Storm Limit:  64 Kbits/second
  Flow Control:           Disabled
  VLAN Trunking:          Disabled
  LACP:                   Disabled
  Port Security:          Disabled
  Max MAC Count:          0
  Port Security Action:   None
  Media Type:             SFP preferred auto
  Port Security          : Disabled
  Max MAC Count          : 0
  Port Security Action   : None
  Media Type             : Copper forced
  Giga PHY mode: Auto preferred master
 Current Status:
  Link Status:            Up
  Port Operation Status:  Up
```

```
  Operation Speed-duplex: 100full
  Port Uptime:            0w  0d  0h   0m  14s (14 seconds)
  Flow Control Type:      None
Console#
```

show interfaces switchport

This command displays the administrative and operational status of the specified interfaces.

SYNTAX

show interfaces switchport [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

Shows all interfaces.

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

If no interface is specified, information on all interfaces is displayed.

EXAMPLE

This example shows the configuration setting for port 1.

```
Console#show interfaces switchport ethernet 1/1
 Broadcast Threshold:           Enabled, 256 Kbits/second
 Multicast Threshold:           Enabled, 256 Kbits/second
 Unknown-unicast Threshold:     Enabled, 256 Kbits/second
 LACP Status:                   Disabled
 Ingress Rate Limit:            Disabled, 100000 Kbits per second
 Egress Rate Limit:             Disabled, 100000 Kbits per second
 VLAN Membership Mode:          Hybrid
 Ingress Rule:                  Enabled
 Acceptable Frame Type:         All frames
 Native VLAN:                   1
 Priority for Untagged Traffic: 0
 GVRP Status:                   Disabled
 Allowed VLAN:                     1(u),4093(t),
 Forbidden VLAN:
 Private-VLAN Mode:             NONE
 Private-VLAN host-association: NONE
 Private-VLAN Mapping:          NONE
 802.1Q-tunnel Status:          Disable
 802.1Q-tunnel Mode:            NORMAL
 802.1Q-tunnel TPID:            8100(Hex)
 Layer 2 Protocol Tunnel:       None
Console#
```

Table 91: show interfaces switchport - display description

Field	Description
Broadcast Threshold	Shows if broadcast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 690).
Multicast Threshold	Shows if multicast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 690).
Unknown-unicast Threshold	Shows if unknown unicast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 690).
LACP Status	Shows if Link Aggregation Control Protocol has been enabled or disabled (page 703).
Ingress/Egress Rate Limit	Shows if rate limiting is enabled, and the current rate limit (page 717).
VLAN Membership Mode	Indicates membership mode as Trunk or Hybrid (page 810).
Ingress Rule	Shows if ingress filtering is enabled or disabled (page 809).
Acceptable Frame Type	Shows if acceptable VLAN frames include all types or tagged frames only (page 807).
Native VLAN	Indicates the default Port VLAN ID (page 811).
Priority for Untagged Traffic	Indicates the default priority for untagged frames (page 848).
GVRP Status	Shows if GARP VLAN Registration Protocol is enabled or disabled (page 802).
Allowed VLAN	Shows the VLANs this interface has joined, where "(u)" indicates untagged and "(t)" indicates tagged (page 808).
Forbidden VLAN	Shows the VLANs this interface can not dynamically join via GVRP (page 802).
Private-VLAN Mode	Shows the private VLAN mode as host, promiscuous, or none (page 828).
Private VLAN host-association	Shows the secondary (or community) VLAN with which this port is associated (page 828).
Private VLAN mapping	Shows the primary VLAN mapping for a promiscuous port (page 829).
802.1Q-tunnel Status	Shows if 802.1Q tunnel is enabled on this interface (page 815).
802.1Q-tunnel Mode	Shows the tunnel mode as Normal, 802.1Q Tunnel or 802.1Q Tunnel Uplink (page 816).
802.1Q-tunnel TPID	Shows the Tag Protocol Identifier used for learning and switching packets (page 818).
Layer 2 Protocol Tunnel	Shows if L2 Protocol Tunnel is enabled for spanning tree protocol (page 820).

show interfaces transceiver

This command displays identifying information for the specified transceiver, as well as the temperature, voltage, bias current, transmit power, and receive power.

SYNTAX

show interfaces transceiver [*interface*]

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

Shows all SFP interfaces.

COMMAND MODE

Privileged Exec

COMMAND USAGE

The switch can display diagnostic information for SFP modules which support the SFF-8472 Specification for Diagnostic Monitoring Interface for Optical Transceivers. This information allows administrators to remotely diagnose problems with optical devices.

EXAMPLE

```
Console#show interfaces transceiver ethernet 1/27
Information of Eth 1/27
 Connector Type        : LC
 Fiber Type            : Single Mode (SM)
 Eth Compliance Codes  : 1000BASE-LX
 Tx Central Wavelength : 1310 nm
 Baud Rate             : 1300 MBd
 Vendor OUI            : 00-00-00
 Vendor Name           : DELTA
 Vendor PN             : LCP-1250B4QDRT
 Vendor Rev            : 000
 Vendor SN             : 0000070904100004
 Date Code             : 07-03-02
 Temperature           : 40 degrees C
 Vcc                   : 3.36 V
 Bias Current          : 21.92 mA
 TX Power              : 270 uW
 RX Power              : 0 uW
Console#
```

test cable-diagnostics tdr interface

This command performs cable diagnostics on the specified port to diagnose any cable faults (short, open, etc.) and report the cable length.

SYNTAX

test cable-diagnostics tdr interface *interface*

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

COMMAND MODE

Privileged Exec

COMMAND USAGE

- Cable diagnostics are performed using Time Domain Reflectometry (TDR) test methods.
- This cable test is only accurate for cables 7 - 140 meters long.
- The test takes approximately 5 seconds. The switch displays the results of the test immediately upon completion, including common cable failures, as well as the status and approximate length of each cable pair.
- Potential conditions which may be listed by the diagnostics include:
  - OK: Correctly terminated pair
  - Open: Open pair, no link partner
  - Short: Shorted pair
  - Impedance mismatch: Terminating impedance is not in the reference range.
- Ports are linked down while running cable diagnostics.

EXAMPLE

```
Console#test cable-diagnostics tdr interface ethernet 1/1
Port     Type  Link Status Pair A (meters)  Pair B (meters)  Last Update
-------- ---- ----------- ---------------- ---------------- -------------------
Eth 1/ 1  FE  Up          OK (0)           OK (0)           2001-01-01 08:25:32
Console#
```

show cable-diagnostics

This command shows the results of a cable diagnostics test.

SYNTAX

show cable-diagnostics interface [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show cable-diagnostics tdr interface ethernet 1/1
Port     Type  Link Status Pair A (meters)  Pair B (meters)  Last Update
-------- ---- ----------- ---------------- ---------------- -------------------
Eth 1/ 1  FE  Up          OK (0)           OK (0)           2001-01-01 08:25:32
Console#
```

28 LINK AGGREGATION COMMANDS

Ports can be statically grouped into an aggregate link (i.e., trunk) to increase the bandwidth of a network connection or to ensure fault recovery. Or you can use the Link Aggregation Control Protocol (LACP) to automatically negotiate a trunk link between this switch and another network device. For static trunks, the switches have to comply with the Cisco EtherChannel standard. For dynamic trunks, the switches have to comply with LACP. This switch supports up to 5 trunks. For example, a trunk consisting of two 1000 Mbps ports can support an aggregate bandwidth of 4 Gbps when operating at full duplex.

Table 92: Link Aggregation Commands

Command	Function	Mode
Manual Configuration Commands		
interface port-channel	Configures a trunk and enters interface configuration mode for the trunk	GC
channel-group	Adds a port to a trunk	IC (Ethernet)
Dynamic Configuration Commands		
lacp	Configures LACP for the current interface	IC (Ethernet)
lacp admin-key	Configures a port's administration key	IC (Ethernet)
lacp mode	Configures active or passive LACP initiation mode	IC (Ethernet)
lacp port-priority	Configures a port's LACP port priority	IC (Ethernet)
lacp system-priority	Configures a port's LACP system priority	IC (Ethernet)
lacp admin-key	Configures an port channel's administration key	IC (Port Channel)
Trunk Status Display Commands		
show interfaces status port-channel	Shows trunk information	NE, PE
show lacp	Shows LACP information	PE

GUIDELINES FOR CREATING TRUNKS

General Guidelines –

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- A trunk can have up to 8 ports.
- The ports at both ends of a connection must be configured as trunk ports.
- All ports in a trunk must be configured in an identical manner, including communication mode (i.e., speed and duplex mode), VLAN assignments, and CoS settings.

- Any of the 100BASE-TX ports can be trunked together. Any of the Gigabit ports (Ports 25-28/49-52) on the front panel can also be trunked together, including ports of different media types.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN via the specified port-channel.
- STP, VLAN, and IGMP settings can only be made for the entire trunk via the specified port-channel.

Dynamically Creating a Port Channel –

Ports assigned to a common port channel must meet the following criteria:

- Ports must have the same LACP system priority.
- Ports must have the same port admin key (Ethernet Interface).
- If the port channel admin key (lacp admin key - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (lacp admin key - Ethernet Interface) used by the interfaces that joined the group.
- However, if the port channel admin key is set, then the port admin key must be set to the same value for a port to be allowed to join a channel group.
- If a link goes down, LACP port priority is used to select the backup link.

channel-group

This command adds a port to a trunk. Use the **no** form to remove a port from a trunk.

SYNTAX

channel-group *channel-id*

no channel-group

channel-id - Trunk index (Range: 1-8)

DEFAULT SETTING

The current port will be added to this trunk.

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- When configuring static trunks, the switches must comply with the Cisco EtherChannel standard.
- Use **no channel-group** to remove a port group from a trunk.
- Use no interface port-channel to remove a trunk from the switch.

EXAMPLE

The following example creates trunk 1 and then adds port 10:

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/10
Console(config-if)#channel-group 1
Console(config-if)#
```

lacp

This command enables Link Aggregation Control Protocol (LACP) for the current interface. Use the **no** form to disable it.

SYNTAX

[**no**] **lacp**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- The ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.
- A trunk formed with another switch using LACP will automatically be assigned the next available port-channel ID.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.

EXAMPLE

The following shows LACP enabled on ports 1-3. Because LACP has also been enabled on the ports at the other end of the links, the show interfaces status port-channel 1 command shows that Trunk1 has been established.

```
Console(config)#interface ethernet 1/1
Console(config-if)#lacp
Console(config-if)#interface ethernet 1/2
Console(config-if)#lacp
Console(config-if)#interface ethernet 1/3
Console(config-if)#lacp
Console(config-if)#end
```

```
Console#show interfaces status port-channel 1
Information of Trunk 1
 Basic Information:
  Port Type:              100TX
  Mac Address:            00-12-CF-61-24-37
 Configuration:
  Name:
  Port Admin:             Up
  MDIX mode:              Auto
  Speed-duplex:           Auto
  Capabilities:           10half, 10full, 100half, 100full
  Flow Control:           Disabled
  VLAN Trunking:          Disabled
  Port Security:          Disabled
  Max MAC Count:          0
  Giga PHY mode: Auto preferred master
 Current Status:
  Created By:             LACP
  Link Status:            Up
  Port Operation Status:  Up
  Operation Speed-duplex: 100full
  Trunk Uptime:            0w  0d  0h   0m  55s (55 seconds)
  Flow Control Type:      None
  Member Ports: Eth1/1, Eth1/2, Eth1/3,
Console#
```

lacp admin-key (Ethernet Interface)

This command configures a port's LACP administration key. Use the **no** form to restore the default setting.

SYNTAX

lacp {**actor** | **partner**} **admin-key** *key*

no lacp {**actor** | **partner**} **admin-key**

actor - The local side an aggregate link.

partner - The remote side of an aggregate link.

key - The port admin key must be set to the same value for ports that belong to the same link aggregation group (LAG). (Range: 0-65535)

DEFAULT SETTING

0

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).
- If the port channel admin key (lacp admin key - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (**lacp admin key** - Ethernet Interface) used by the interfaces that joined the group.

- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor admin-key 120
Console(config-if)#
```

lacp mode

This command configures active or passive LACP initiation mode. Use the **no** form to restore the default setting.

SYNTAX

lacp mode {**actor** | **partner**} {**active** | **passive**}

no lacp mode {**actor** | **partner**}

actor - The local side of an aggregate link.

partner - The remote side of an aggregate link.

active - Enables active initiation of LACP negotiation on a port, automatically sending LACP negotiation packets.

passive - Enables passive initiation of LACP negotiation on a port, which starts negotiations only if an LACP device is detected at the other end of the link.

DEFAULT SETTING

active

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

Regardless of the LACP initiation mode, if the target switch has also enabled LACP on the connected ports and negotiations are successfully completed, the trunk will be activated automatically.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp mode actor active
Console(config-if)#
```

lacp port-priority

This command configures LACP port priority. Use the **no** form to restore the default setting.

SYNTAX

lacp {**actor** | **partner**} **port-priority** *priority*

no lacp {**actor** | **partner**} **port-priority**

actor - The local side an aggregate link.

partner - The remote side of an aggregate link.

priority - LACP port priority is used to select a backup link. (Range: 0-65535)

DEFAULT SETTING

32768

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- Setting a lower value indicates a higher effective priority.
- If an active port link goes down, the backup port with the highest priority is selected to replace the downed link. However, if two or more ports have the same LACP port priority, the port with the lowest physical port number will be selected as the backup port.
- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor port-priority 128
```

lacp system-priority

This command configures a port's LACP system priority. Use the **no** form to restore the default setting.

SYNTAX

lacp {**actor** | **partner**} **system-priority** *priority*

no lacp {**actor** | **partner**} **system-priority**

actor - The local side an aggregate link.

partner - The remote side of an aggregate link.

priority - This priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535)

DEFAULT SETTING

32768

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- Port must be configured with the same system priority to join the same LAG.
- System priority is combined with the switch's MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.
- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor system-priority 3
Console(config-if)#
```

lacp admin-key (Port Channel)

This command configures a port channel's LACP administration key string. Use the **no** form to restore the default setting.

SYNTAX

lacp admin-key *key*

no lacp admin-key

key - The port channel admin key is used to identify a specific link aggregation group (LAG) during local LACP setup on this switch. (Range: 0-65535)

DEFAULT SETTING
0

COMMAND MODE
Interface Configuration (Port Channel)

COMMAND USAGE
- Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).
- If the port channel admin key (**lacp admin key** - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (lacp admin key - Ethernet Interface) used by the interfaces that joined the group. Note that when the LAG is no longer used, the port channel admin key is reset to 0.

EXAMPLE
```
Console(config)#interface port-channel 1
Console(config-if)#lacp admin-key 3
Console(config-if)#
```

show lacp
This command displays LACP information.

SYNTAX
show lacp [*port-channel*] {**counters** | **internal** | **neighbors** | **sys-id**}

port-channel - Local identifier for a link aggregation group. (Range: 1-8)

counters - Statistics for LACP protocol messages.

internal - Configuration settings and operational state for local side.

neighbors - Configuration settings and operational state for remote side.

sys-id - Summary of system priority and MAC address for all channel groups.

DEFAULT SETTING
Port Channel: all

COMMAND MODE
Privileged Exec

EXAMPLE

```
Console#show lacp 1 counters
Port Channel: 1
-------------------------------------------------------------------------------
Eth 1/ 2
-------------------------------------------------------------------------------
  LACPDUs Sent:         52
  LACPDUs Received:     41
  Marker Sent:          0
  Marker Received:      0
  LACPDUs Unknown Pkts: 0
  LACPDUs Illegal Pkts: 0
⋮
```

Table 93: show lacp counters - display description

Field	Description
LACPDUs Sent	Number of valid LACPDUs transmitted from this channel group.
LACPDUs Received	Number of valid LACPDUs received on this channel group.
Marker Sent	Number of valid Marker PDUs transmitted from this channel group.
Marker Received	Number of valid Marker PDUs received by this channel group.
LACPDUs Unknown Pkts	Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.
LACPDUs Illegal Pkts	Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.

```
Console#show lacp 1 internal
Port Channel : 1
-------------------------------------------------------------------------------
Oper Key:  3
Admin Key: 0
Eth 1/ 1
-------------------------------------------------------------------------------
  LACPDUs Internal:     30 sec
  LACP System Priority: 32768
  LACP Port Priority:   32768
  Admin Key:            3
  Oper Key:             3
  Admin State: defaulted, aggregation, long timeout, active
  Oper State:           distributing, collecting, synchronization,
                        aggregation, long timeout, active
⋮
```

Table 94: show lacp internal - display description

Field	Description
Oper Key	Current operational value of the key for the aggregation port.
Admin Key	Current administrative value of the key for the aggregation port.
LACPDUs Internal	Number of seconds before invalidating received LACPDU information.
LACP System Priority	LACP system priority assigned to this port channel.

Table 94: show lacp internal - display description (Continued)

Field	Description
LACP Port Priority	LACP port priority assigned to this interface within the channel group.
Admin State, Oper State	Administrative or operational values of the actor's state parameters: ◆ Expired – The actor's receive machine is in the expired state; ◆ Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner. ◆ Distributing – If false, distribution of outgoing frames on this link is disabled; i.e., distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information. ◆ Collecting – Collection of incoming frames on this link is enabled; i.e., collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. ◆ Synchronization – The System considers this link to be IN_SYNC; i.e., it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted. ◆ Aggregation – The system considers this link to be aggregatable; i.e., a potential candidate for aggregation. ◆ Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate. ◆ LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active)

```
Console#show lacp 1 neighbors
Port Channel 1 neighbors
------------------------------------------------------------------------
Eth 1/ 1
------------------------------------------------------------------------
  Partner Admin System ID:   32768, 00-00-00-00-00-00
  Partner Oper System ID:    32768, 00-12-CF-DA-FC-E8
  Partner Admin Port Number: 8
  Partner Oper Port Number:  8
  Port Admin Priority:       32768
  Port Oper Priority:        32768
  Admin Key:                 0
  Oper Key:                  3
  Admin State:               defaulted, distributing, collecting,
                             synchronization, long timeout,
  Oper State:                distributing, collecting, synchronization,
                             aggregation, long timeout, active
⋮
```

Table 95: show lacp neighbors - display description

Field	Description
Partner Admin System ID	LAG partner's system ID assigned by the user.
Partner Oper System ID	LAG partner's system ID assigned by the LACP protocol.
Partner Admin Port Number	Current administrative value of the port number for the protocol Partner.

Table 95: show lacp neighbors - display description (Continued)

Field	Description
Partner Oper Port Number	Operational port number assigned to this aggregation port by the port's protocol partner.
Port Admin Priority	Current administrative value of the port priority for the protocol partner.
Port Oper Priority	Priority value assigned to this aggregation port by the partner.
Admin Key	Current administrative value of the Key for the protocol partner.
Oper Key	Current operational value of the Key for the protocol partner.
Admin State	Administrative values of the partner's state parameters. (See preceding table.)
Oper State	Operational values of the partner's state parameters. (See preceding table.)

```
 Console#show lacp sysid
Port Channel     System Priority    System MAC Address
-------------------------------------------------------------------------
           1              32768     00-30-F1-8F-2C-A7
           2              32768     00-30-F1-8F-2C-A7
           3              32768     00-30-F1-8F-2C-A7
           4              32768     00-30-F1-8F-2C-A7
           5              32768     00-30-F1-8F-2C-A7
           6              32768     00-30-F1-8F-2C-A7
           7              32768     00-30-F1-D4-73-A0
           8              32768     00-30-F1-D4-73-A0
           9              32768     00-30-F1-D4-73-A0
          10              32768     00-30-F1-D4-73-A0
          11              32768     00-30-F1-D4-73-A0
          12              32768     00-30-F1-D4-73-A0
⋮
```

Table 96: show lacp sysid - display description

Field	Description
Channel group	A link aggregation group configured on this switch.
System Priority*	LACP system priority for this channel group.
System MAC Address*	System MAC address.

* The LACP system priority and system MAC address are concatenated to form the LAG system ID.

29 PORT MIRRORING COMMANDS

Data can be mirrored from a local port on the same switch for analysis at the target port using software monitoring tools or a hardware probe.

This section describes how to mirror traffic from a source port to a target port.

Table 97: Mirror Port Commands

Command	Function	Mode
port monitor	Configures a mirror session	IC
show port monitor	Shows the configuration for a mirror port	PE

port monitor

This command configures a mirror session. Use the **no** form to clear a mirror session.

SYNTAX

port monitor {*interface* [**rx** | **tx** | **both**] | **vlan** *vlan-id* | **mac-address** *mac-address*}

no port monitor *interface*

interface - **ethernet** *unit*/*port* (source port)

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

rx - Mirror received packets.

tx - Mirror transmitted packets.

both - Mirror both received and transmitted packets.

vlan-id - VLAN ID (Range: 1-4094)

mac-address - MAC address in the form of xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.

DEFAULT SETTING

- No mirror session is defined.
- When enabled for an interface, default mirroring is for both received and transmitted packets.
- When enabled for a VLAN or a MAC address, mirroring is restricted to received packets.

COMMAND MODE
Interface Configuration (Ethernet, destination port)

COMMAND USAGE
- You can mirror traffic from any source port to a destination port for real-time analysis. You can then attach a logic analyzer or RMON probe to the destination port and study the traffic crossing the source port in a completely unobtrusive manner.
- Set the destination port by specifying an Ethernet interface with the interface configuration command, and then use the **port monitor** command to specify the source of the traffic to mirror.
- When mirroring traffic from a port, the mirror port and monitor port speeds should match, otherwise traffic may be dropped from the monitor port. When mirroring traffic from a VLAN, traffic may also be dropped under heavy loads.
- When VLAN mirroring and port mirroring are both enabled, the target port can receive a mirrored packet twice; once from the source mirror port and again from the source mirror VLAN.
- When mirroring traffic from a MAC address, ingress traffic with the specified source address entering any port in the switch, other than the target port, will be mirrored to the destination port.
- Spanning Tree BPDU packets are not mirrored to the target port.
- You can create multiple mirror sessions, but all sessions must share the same destination port.

EXAMPLE
The following example configures the switch to mirror all packets from port 6 to 5:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port monitor ethernet 1/6 both
Console(config-if)#
```

show port monitor

This command displays mirror information.

SYNTAX
show port monitor [*interface*]

interface - **ethernet** *unit*/*port* (source port)

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

DEFAULT SETTING
Shows all sessions.

COMMAND MODE
Privileged Exec

COMMAND USAGE
This command displays the currently configured source port, destination port, and mirror mode (i.e., RX, TX, RX/TX). When the source is a VLAN, only the destination port and source VLAN are displayed. When the source is a MAC address, only the destination port and MAC address are displayed.

EXAMPLE
The following shows mirroring configured from port 6 to port 5:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port monitor ethernet 1/6 both
Console(config-if)#end
Console#show port monitor
Port Mirroring
-------------------------------------
 Destination Port (listen port):Eth1/5
 Source Port (monitored port)  :Eth1/6
 Mode                          :RX/TX
Console#
```

30 RATE LIMIT COMMANDS

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped.

Table 98: Rate Limit Commands

Command	Function	Mode
rate-limit	Configures the maximum input or output rate for an interface	IC

rate-limit

This command defines the rate limit for a specific interface. Use this command without specifying a rate to restore the default rate. Use the **no** form to restore the default status of disabled.

SYNTAX

rate-limit {**input** | **output**} [*rate*]

no rate-limit {**input** | **output**}

input – Input rate for specified interface

output – Output rate for specified interface

rate – Maximum value in Kbps.
(Range: 64-100000 Kbps for Fast Ethernet ports,
64-1000000 Kbps for Gigabit Ethernet ports)

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

Using both rate limiting and storm control on the same interface may lead to unexpected results. For example, suppose broadcast storm control is set to 500 Kbps by the command "switchport broadcast packet-rate 500," and the rate limit is set to 20000 Kbps by the command "rate-limit input 20000" on a Fast Ethernet port. Since 20000 Kbps is 1/5 of line speed (100 Mbps), the received rate will actually be 100 Kbps, or 1/5 of the 500 Kbps limit set

by the storm control command. It is therefore not advisable to use both of these commands on the same interface.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input 64
Console(config-if)#
```

RELATED COMMAND

show interfaces switchport (695)

31 AUTOMATIC TRAFFIC CONTROL COMMANDS

Automatic Traffic Control (ATC) configures bounding thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port.

Table 99: ATC Commands

Command	Function	Mode
Threshold Commands		
auto-traffic-control apply-timer	Sets the time at which to apply the control response after ingress traffic has exceeded the upper threshold	GC
auto-traffic-control release-timer	Sets the time at which to release the control response after ingress traffic has fallen beneath the lower threshold	GC
auto-traffic-control*	Enables automatic traffic control for broadcast or multicast storms	IC (Port)
auto-traffic-control action	Sets the control action to limit ingress traffic or shut down the offending port	IC (Port)
auto-traffic-control alarm-clear-threshold	Sets the lower threshold for ingress traffic beneath which a cleared storm control trap is sent	IC (Port)
auto-traffic-control alarm-fire-threshold	Sets the upper threshold for ingress traffic beyond which a storm control response is triggered after the apply timer expires	IC (Port)
auto-traffic-control control-release	Manually releases a control response	IC (Port)
auto-traffic-control auto-control-release	Automatically releases a control response	PE
SNMP Trap Commands		
snmp-server enable port-traps atc broadcast-alarm-clear	Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered	IC (Port)
snmp-server enable port-traps atc broadcast-alarm-fire	Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control	IC (Port)
snmp-server enable port-traps atc broadcast-control-apply	Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control and the apply timer expires	IC (Port)
snmp-server enable port-traps atc broadcast-control-release	Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires	IC (Port)
snmp-server enable port-traps atc multicast-alarm-clear	Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered	IC (Port)
snmp-server enable port-traps atc multicast-alarm-fire	Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control	IC (Port)

Table 99: ATC Commands (Continued)

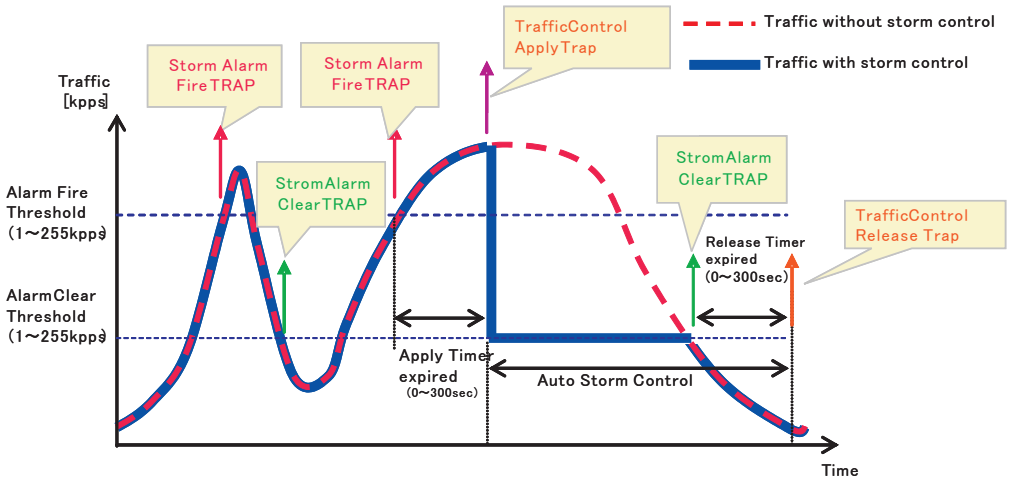
Command	Function	Mode
snmp-server enable port-traps atc multicast-control-apply	Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control and the apply timer expires	IC (Port)
snmp-server enable port-traps atc multicast-control-release	Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires	IC (Port)
ATC Display Commands		
show auto-traffic-control	Shows global configuration settings for automatic storm control	PE
show auto-traffic-control interface	Shows interface configuration settings and storm control status for the specified port	PE

* Enabling automatic storm control on a port will disable hardware-level storm control on the same port if configured by the switchport packet-rate command.

USAGE GUIDELINES

ATC includes storm control for broadcast or multicast traffic. The control response for either of these traffic types is the same, as shown in the following diagrams.

Figure 216: Storm Control by Limiting the Traffic Rate



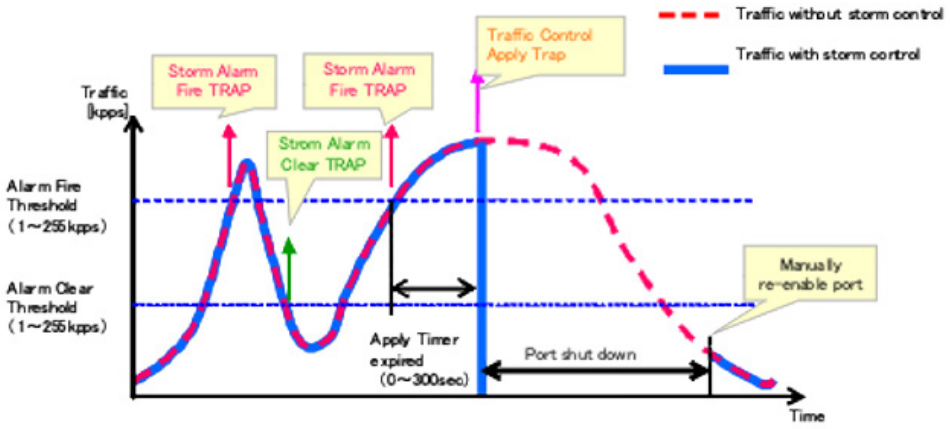
The key elements of this diagram are described below:

- Alarm Fire Threshold – The highest acceptable traffic rate. When ingress traffic exceeds the threshold, ATC sends a Storm Alarm Fire Trap and logs it.
- When traffic exceeds the alarm fire threshold and the apply timer expires, a traffic control response is applied, and a Traffic Control Apply Trap is sent and logged.
- Alarm Clear Threshold – The lower threshold beneath which an control response can be automatically terminated after the release timer

expires. When ingress traffic falls below this threshold, ATC sends a Storm Alarm Clear Trap and logs it.

- When traffic falls below the alarm clear threshold after the release timer expires, traffic control will be stopped and a Traffic Control Release Trap sent and logged.
- The traffic control response of rate limiting can be released automatically or manually. The control response of shutting down a port can only be released manually.

Figure 217: Storm Control by Shutting Down a Port



The key elements of this diagram are the same as that described in the preceding diagram, except that automatic release of the control response is not provided. When traffic control is applied, you must manually re-enable the port.

FUNCTIONAL LIMITATIONS

Automatic storm control is a software level control function. Traffic storms can also be controlled at the hardware level using the switchport packet-rate command. However, only one of these control types can be applied to a port. Enabling automatic storm control on a port will disable hardware-level storm control on that port.

auto-traffic-control apply-timer

This command sets the time at which to apply the control response after ingress traffic has exceeded the upper threshold. Use the **no** form to restore the default setting.

SYNTAX

auto-traffic-control {**broadcast** | **multicast**} **apply-timer** *seconds*

no auto-traffic-control {**broadcast** | **multicast**} **apply-timer**

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

seconds - The interval after the upper threshold has been exceeded at which to apply the control response. (Range: 1-300 seconds)

DEFAULT SETTING
300 seconds

COMMAND MODE
Global Configuration

COMMAND USAGE
After the apply timer expires, a control action may be triggered as specified by the auto-traffic-control action command and a trap message sent as specified by the snmp-server enable port-traps atc broadcast-control-apply command or snmp-server enable port-traps atc multicast-control-apply command.

EXAMPLE
This example sets the apply timer to 200 seconds for all ports.

```
Console(config)#auto-traffic-control broadcast apply-timer 200
Console(config)#
```

auto-traffic-control release-timer

This command sets the time at which to release the control response after ingress traffic has fallen beneath the lower threshold. Use the **no** form to restore the default setting.

SYNTAX

auto-traffic-control {**broadcast** | **multicast**}
release-timer *seconds*

no auto-traffic-control {**broadcast** | **multicast**} **release-timer**

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

seconds - The time at which to release the control response after ingress traffic has fallen beneath the lower threshold.
(Range: 1-900 seconds)

DEFAULT SETTING
900 seconds

COMMAND MODE
Global Configuration

COMMAND USAGE
This command sets the delay after which the control response can be terminated. The auto-traffic-control auto-control-release command must be used to enable or disable the automatic release.

EXAMPLE

This example sets the release timer to 800 seconds for all ports.

```
Console(config)#auto-traffic-control broadcast release-timer 800
Console(config)#
```

auto-traffic-control

This command enables automatic traffic control for broadcast or multicast storms. Use the **no** form to disable this feature.

SYNTAX

[**no**] **auto-traffic-control** {**broadcast** | **multicast**}

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- Automatic storm control can be enabled for either broadcast or multicast traffic. It cannot be enabled for both of these traffic types at the same time.
- Automatic storm control is a software level control function. Traffic storms can also be controlled at the hardware level using the switchport packet-rate command. However, only one of these control types can be applied to a port. Enabling automatic storm control on a port will disable hardware-level storm control on that port.

EXAMPLE

This example enables automatic storm control for broadcast traffic on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast
Console(config-if)#
```

auto-traffic-control action

This command sets the control action to limit ingress traffic or shut down the offending port. Use the **no** form to restore the default setting.

SYNTAX

auto-traffic-control {**broadcast** | **multicast**}
action {**rate-control** | **shutdown**}

no auto-traffic-control {**broadcast** | **multicast**} **action**

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

rate-control - If a control response is triggered, the rate of ingress traffic is limited based on the threshold configured by the auto-traffic-control alarm-clear-threshold command.

shutdown - If a control response is triggered, the port is administratively disabled. A port disabled by automatic traffic control can only be manually re-enabled.

DEFAULT SETTING

rate-control

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- When the upper threshold is exceeded and the apply timer expires, a control response will be triggered based on this command.
- When the control response is set to rate limiting by this command, the rate limits are determined by the auto-traffic-control alarm-clear-threshold command.
- If the control response is to limit the rate of ingress traffic, it can be automatically terminated once the traffic rate has fallen beneath the lower threshold and the release timer has expired.
- If a port has been shut down by a control response, it will not be re-enabled by automatic traffic control. It can only be manually re-enabled using the auto-traffic-control control-release command.

EXAMPLE

This example sets the control response for broadcast traffic on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast action shutdown
Console(config-if)#
```

auto-traffic-control alarm-clear-threshold

This command sets the lower threshold for ingress traffic beneath which a cleared storm control trap is sent. Use the **no** form to restore the default setting.

SYNTAX

auto-traffic-control {**broadcast** | **multicast**}
alarm-clear-threshold *threshold*

no auto-traffic-control {**broadcast** | **multicast**}
alarm-clear-threshold

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

threshold - The lower threshold for ingress traffic beneath which a cleared storm control trap is sent. (Range: 1-255 kilo-packets per second seconds)

DEFAULT SETTING

128 kilo-packets per seconds

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- Once the traffic rate falls beneath the lower threshold, a trap message may be sent if configured by the snmp-server enable port-traps atc broadcast-alarm-clear command or snmp-server enable port-traps atc multicast-alarm-clear command.

- If rate limiting has been configured as a control response, it will discontinued after the traffic rate has fallen beneath the lower threshold, and the release timer has expired. Note that if a port has been shut down by a control response, it will not be re-enabled by automatic traffic control. It can only be manually re-enabled using the auto-traffic-control control-release command.

EXAMPLE

This example sets the clear threshold for automatic storm control for broadcast traffic on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast alarm-clear-threshold 155
Console(config-if)#
```

auto-traffic-control alarm-fire-threshold

This command sets the upper threshold for ingress traffic beyond which a storm control response is triggered after the apply timer expires. Use the **no** form to restore the default setting.

SYNTAX

auto-traffic-control {**broadcast** | **multicast**}
alarm-fire-threshold *threshold*

no auto-traffic-control {**broadcast** | **multicast**}
alarm-fire-threshold

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

threshold - The upper threshold for ingress traffic beyond which a storm control response is triggered after the apply timer expires. (Range: 1-255 kilo-packets per second seconds)

DEFAULT SETTING

128 kilo-packets per seconds

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- Once the upper threshold is exceeded, a trap message may be sent if configured by the snmp-server enable port-traps atc broadcast-alarm-fire command or snmp-server enable port-traps atc multicast-alarm-fire command.
- After the upper threshold is exceeded, the control timer must first expire as configured by the auto-traffic-control apply-timer command before a control response is triggered if configured by the auto-traffic-control action command.

EXAMPLE

This example sets the trigger threshold for automatic storm control for broadcast traffic on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast alarm-fire-threshold 255
Console(config-if)#
```

auto-traffic-control control-release

This command manually releases a control response.

SYNTAX

auto-traffic-control {**broadcast** | **multicast**} **control-release**

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

COMMAND MODE
Privileged Exec

COMMAND USAGE
This command can be used to manually stop a control response any time after the specified action has been triggered.

EXAMPLE

```
Console#auto-traffic-control broadcast control-release interface ethernet 1/1
Console#
```

auto-traffic-control auto-control-release

This command automatically releases a control response after the time specified in the auto-traffic-control release-timer command has expired.

SYNTAX

auto-traffic-control {**broadcast** | **multicast**}
auto-control-release

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

COMMAND MODE
Interface Configuration (Ethernet)

COMMAND USAGE
This command can be used to automatically stop a control response after the specified action has been triggered and the release timer has expired.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast auto-control-release
Console(config-if)#
```

snmp-server enable port-traps atc broadcast-alarm-clear

This command sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered. Use the **no** form to disable this trap.

SYNTAX

[**no**] **snmp-server enable port-traps atc broadcast-alarm-clear**

DEFAULT SETTING
Disabled

COMMAND MODE
Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-alarm-clear
Console(config-if)#
```

RELATED COMMANDS

auto-traffic-control action (724)
auto-traffic-control alarm-clear-threshold (725)

snmp-server enable port-traps atc broadcast-alarm-fire

This command sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control. Use the **no** form to disable this trap.

SYNTAX

[**no**] **snmp-server enable port-traps atc broadcast-alarm-fire**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-alarm-fire
Console(config-if)#
```

RELATED COMMANDS

auto-traffic-control alarm-fire-threshold (726)

snmp-server enable port-traps atc broadcast-control-apply

This command sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control and the apply timer expires. Use the **no** form to disable this trap.

SYNTAX

[**no**] **snmp-server enable port-traps atc broadcast-control-apply**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-control-apply
Console(config-if)#
```

RELATED COMMANDS

auto-traffic-control alarm-fire-threshold (726)
auto-traffic-control apply-timer (721)

snmp-server enable port-traps atc broadcast-control-release

This command sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires. Use the **no** form to disable this trap.

SYNTAX

[**no**] **snmp-server enable port-traps atc broadcast-control-release**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-control-
  release
Console(config-if)#
```

RELATED COMMANDS

auto-traffic-control alarm-clear-threshold (725)
auto-traffic-control action (724)
auto-traffic-control release-timer (722)

snmp-server enable port-traps atc multicast-alarm-clear

This command sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered. Use the **no** form to disable this trap.

SYNTAX

[**no**] **snmp-server enable port-traps atc multicast-alarm-clear**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-alarm-clear
Console(config-if)#
```

RELATED COMMANDS

auto-traffic-control action (724)
auto-traffic-control alarm-clear-threshold (725)

snmp-server enable port-traps atc multicast-alarm-fire

This command sends a trap when multicast traffic exceeds the upper threshold for automatic storm control. Use the **no** form to disable this trap.

SYNTAX

[**no**] **snmp-server enable port-traps atc multicast-alarm-fire**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-alarm-fire
Console(config-if)#
```

RELATED COMMANDS

auto-traffic-control alarm-fire-threshold (726)

snmp-server enable port-traps atc multicast-control-apply

This command sends a trap when multicast traffic exceeds the upper threshold for automatic storm control and the apply timer expires. Use the **no** form to disable this trap.

SYNTAX

[**no**] **snmp-server enable port-traps atc multicast-control-apply**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-control-apply
Console(config-if)#
```

RELATED COMMANDS

auto-traffic-control alarm-fire-threshold (726)
auto-traffic-control apply-timer (721)

snmp-server enable port-traps atc multicast-control-release

This command sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires. Use the **no** form to disable this trap.

SYNTAX

[**no**] **snmp-server enable port-traps atc multicast-control-release**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-control-
  release
Console(config-if)#
```

RELATED COMMANDS

auto-traffic-control alarm-clear-threshold (725)
auto-traffic-control action (724)
auto-traffic-control release-timer (722)

show auto-traffic-control

This command shows global configuration settings for automatic storm control.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show auto-traffic-control

Storm-control: Broadcast
 Apply-timer (sec)    : 300
 release-timer (sec) : 900
```

```
Storm-control: Multicast
 Apply-timer(sec)     : 300
 release-timer(sec)   : 900
Console#
```

show auto-traffic-control interface

This command shows interface configuration settings and storm control status for the specified port.

SYNTAX

show auto-traffic-control interface [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show auto-traffic-control interface ethernet 1/1
Eth 1/1 Information
---------------------------------------------------------------------------
Storm Control:              Broadcast                   Multicast
State:                      Disabled                    Disabled
Action:                     rate-control                rate-control
Auto Release Control:       Disabled                    Disabled
Alarm Fire Threshold(Kpps): 128                         128
Alarm Clear Threshold(Kpps):128                         128
Trap Storm Fire:            Disabled                    Disabled
Trap Storm Clear:           Disabled                    Disabled
Trap Traffic Apply:         Disabled                    Disabled
Trap Traffic Release:       Disabled                    Disabled
---------------------------------------------------------------------------

Console#
```

32 LOOPBACK DETECTION COMMANDS

The switch can be configured to detect general loopback conditions caused by hardware problems or faulty protocol settings. When enabled, a control frame is transmitted on the participating ports, and the switch monitors inbound traffic to see if the frame is looped back.

Table 100: Loopback Detection Commands

Command	Function	Mode
loopback-detection	Enables loopback detection globally on the switch or on a specified interface	GC, IC
loopback-detection mode	Specifies shutdown by dropping packets for ports detected in loopback state or by dropping packets belonging to VLANs detected in loopback state	GC
loopback-detection recover-time	Specifies the interval to wait before releasing an interface from shutdown state	GC
loopback-detection transmit-interval	Specifies the interval at which to transmit loopback detection control frames	GC
loopback-detection release	Manually releases all interfaces currently shut down by the loopback detection feature	PE
show loopback-detection	Shows loopback detection configuration settings for the switch or for a specified interface	PE

USAGE GUIDELINES

- The default settings for the control frame transmit interval and recover time may be adjusted to improve performance for your specific environment. The shutdown mode may also need to be changed once you determine what kind of packets are being looped back.
- General loopback detection provided by the command described in this section and loopback detection provided by the spanning tree protocol cannot both be enabled at the same time. If loopback detection is enabled for the spanning tree protocol, general loopback detection cannot be enabled on the same interface.
- When a loopback event is detected on an interface or when a interface is released from a shutdown state caused by a loopback event, a trap message is sent and the event recorded in the system log.
- Loopback detection must be enabled both globally and on an interface for loopback detection to take effect.

loopback-detection

This command enables loopback detection globally on the switch or on a specified interface. Use the **no** form to disable loopback detection.

SYNTAX

[**no**] **loopback-detection**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration
Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

Loopback detection must be enabled globally for the switch by this command and enabled for a specific interface for this function to take effect.

EXAMPLE

This example enables general loopback detection on the switch, disables loopback detection provided for the spanning tree protocol on port 1, and then enables general loopback detection for that port.

```
Console(config)#loopback-detection
Console(config)#interface ethernet 1/1
Console(config-if)#no spanning-tree loopback-detection
Console(config-if)#loopback-detection
Console(config)#
```

loopback-detection mode

This command specifies shutdown by dropping packets for a port detected in loopback state or by dropping packets belonging to a VLAN detected in loopback state. Use the **no** form to restore the default setting.

SYNTAX

loopback-detection mode {**port-based** | **vlan-based**}

no loopback-detection mode

port-based - When loopback is detected on a port, the port is shut down automatically.

vlan-based - When loopback is detected on a port which a member of a specific VLAN, packets belonging to that VLAN are dropped at the port.

DEFAULT SETTING

port-based

COMMAND MODE

Global Configuration

COMMAND USAGE

- When using vlan-based mode, loopback detection control frames are untagged or tagged depending on the port's VLAN membership type.
- When using vlan-based mode, ingress filtering for the port is enabled automatically if not already enabled by the switchport ingress-filtering command. The port's original setting for ingress filtering will be restored when loopback detection is disabled.
- When the loopback detection mode is changed, any ports placed in shutdown state by the loopback detection process will be immediately restored to operation regardless of the remaining recover time.

EXAMPLE

This example sets the loopback detection mode to VLAN based.

```
Console(config)#loopback-detection mode vlan-based
Console(config)#
```

loopback-detection recover-time

This command specifies the interval to wait before the switch automatically releases an interface from shutdown state. Use the **no** form to restore the default setting.

SYNTAX

loopback-detection recover-time *seconds*

no loopback-detection recover-time

seconds - Recovery time from shutdown state.
(Range: 60-1,000,000 seconds, or 0 to disable automatic recovery)

DEFAULT SETTING

60 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

- When the loopback detection mode is changed, any ports placed in shutdown state by the loopback detection process will be immediately restored to operation regardless of the remaining recover time.
- If the recovery time is set to zero, all ports placed in shutdown state can be restored to operation using the loopback-detection release command. To restore a specific port, use the no shutdown command.

EXAMPLE

```
Console(config)#loopback-detection recover-time 120
Console(config-if)#
```

loopback-detection transmit-interval

This command specifies the interval at which to transmit loopback detection control frames. Use the **no** form to restore the default setting.

SYNTAX

loopback-detection transmit-interval *seconds*

[**no**] **loopback-detection transmit-interval**

seconds - The transmission interval for loopback detection control frames. (Range: 1-32767 seconds)

DEFAULT SETTING

10 seconds

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#loopback-detection transmit-interval 60
Console(config)#
```

loopback-detection release

This command releases all interfaces currently shut down by the loopback detection feature.

SYNTAX

loopback-detection release

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#loopback-detection release
Console(config)#
```

show loopback-detection

This command shows loopback detection configuration settings for the switch or for a specified interface.

SYNTAX

show loopback-detection [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

COMMAND MODE
Privileged Exec

EXAMPLE

```
Console#show loopback-detection
Loopback Detection Global Information
 Global Status     : Enabled
 Transmit Interval : 10
 Recover Time      : 60
 Mode              : Port-based
Loopback Detection Port Information
 Port      Admin State  Oper State
 --------  -----------  ----------
 Eth 1/ 1  Enabled      Normal
 Eth 1/ 2  Disabled     Disabled
 Eth 1/ 3  Disabled     Disabled
:
Console#show loopback-detection ethernet 1/1
Loopback Detection Information of Eth 1/1
 Admin State : Enabled
 Oper State  : Normal
Console#
```

33 ADDRESS TABLE COMMANDS

These commands are used to configure the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time.

Table 101: Address Table Commands

Command	Function	Mode
mac-address-table aging-time	Sets the aging time of the address table	GC
mac-address-table static	Maps a static address to a port in a VLAN	GC
clear mac-address-table dynamic	Removes any learned entries from the forwarding database	PE
show mac-address-table	Displays entries in the bridge-forwarding database	PE
show mac-address-table aging-time	Shows the aging time for the address table	PE

mac-address-table aging-time

This command sets the aging time for entries in the address table. Use the **no** form to restore the default aging time.

SYNTAX

mac-address-table aging-time *seconds*

no mac-address-table aging-time

seconds - Aging time. (Range: 10-630 seconds; 0 to disable aging)

DEFAULT SETTING

300 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

The aging time is used to age out dynamically learned forwarding information.

EXAMPLE

```
Console(config)#mac-address-table aging-time 100
Console(config)#
```

mac-address-table static

This command maps a static address to a destination port in a VLAN. Use the **no** form to remove an address.

SYNTAX

mac-address-table static *mac-address* **interface** *interface* **vlan** *vlan-id* [*action*]

no mac-address-table static *mac-address* **vlan** *vlan-id*

mac-address - MAC address.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

vlan-id - VLAN ID (Range: 1-4094)

action -

delete-on-reset - Assignment lasts until the switch is reset.

permanent - Assignment is permanent.

DEFAULT SETTING

No static addresses are defined. The default mode is **permanent**.

COMMAND MODE

Global Configuration

COMMAND USAGE

The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

- Static addresses will not be removed from the address table when a given interface link is down.
- Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.
- A static address cannot be learned on another port until the address is removed with the **no** form of this command.

EXAMPLE

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface ethernet
  1/1 vlan 1 delete-on-reset
Console(config)#
```

clear mac-address-table dynamic

This command removes any learned entries from the forwarding database.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#clear mac-address-table dynamic
Console#
```

show mac-address-table

This command shows classes of entries in the bridge-forwarding database.

SYNTAX

show mac-address-table [**address** *mac-address* [*mask*]]
[**interface** *interface*] [**vlan** *vlan-id*]
[**sort** {**address** | **vlan** | **interface**}]

mac-address - MAC address.

mask - Bits to match in the address.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

vlan-id - VLAN ID (Range: 1-4094)

sort - Sort by address, vlan or interface.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

- The MAC Address Table contains the MAC addresses associated with each interface. Note that the Type field may include the following types:
  - Learned - Dynamic address entries
  - Permanent - Static entry
  - Delete-on-reset - Static entry to be deleted when system is reset
- The mask should be hexadecimal numbers (representing an equivalent bit mask) in the form xx-xx-xx-xx-xx-xx that is applied to the specified MAC address. Enter hexadecimal numbers, where an equivalent binary

bit "0" means to match a bit and "1" means to ignore a bit. For example, a mask of 00-00-00-00-00-00 means an exact match, and a mask of FF-FF-FF-FF-FF-FF means "any."

- The maximum number of address entries is 8191.

EXAMPLE

```
Console#show mac-address-table
 Interface MAC Address       VLAN Type
 --------- ----------------- ---- -----------------
  Eth 1/ 1 00-E0-29-94-34-64    1 Learned
  Eth 1/ 1 00-E0-29-94-34-DE    1 Permanent
  Eth 1/ 8 00-12-CF-DA-FC-E8    1 Delete on Reset
Console#
```

show mac-address-table aging-time

This command shows the aging time for entries in the address table.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show mac-address-table aging-time
 Aging Status : Enabled
 Aging Time: 300 sec.
Console#
```

34 SPANNING TREE COMMANDS

This section includes commands that configure the Spanning Tree Algorithm (STA) globally for the switch, and commands that configure STA for the selected interface.

Table 102: Spanning Tree Commands

Command	Function	Mode
spanning-tree	Enables the spanning tree protocol	GC
spanning-tree cisco-prestandard	Configures spanning tree operation to be compatible with Cisco prestandard versions	GC
spanning-tree forward-time	Configures the spanning tree bridge forward time	GC
spanning-tree hello-time	Configures the spanning tree bridge hello time	GC
spanning-tree max-age	Configures the spanning tree bridge maximum age	GC
spanning-tree mode	Configures STP, RSTP or MSTP mode	GC
spanning-tree pathcost method	Configures the path cost method for RSTP/MSTP	GC
spanning-tree priority	Configures the spanning tree bridge priority	GC
spanning-tree mst configuration	Changes to MSTP configuration mode	GC
spanning-tree system-bpdu-flooding	Floods BPDUs to all other ports or just to all other ports in the same VLAN when global spanning tree is disabled	GC
spanning-tree transmission-limit	Configures the transmission limit for RSTP/MSTP	GC
max-hops	Configures the maximum number of hops allowed in the region before a BPDU is discarded	MST
mst priority	Configures the priority of a spanning tree instance	MST
mst vlan	Adds VLANs to a spanning tree instance	MST
name	Configures the name for the multiple spanning tree	MST
revision	Configures the revision number for the multiple spanning tree	MST
spanning-tree bpdu-filter	Filters BPDUs for edge ports	IC
spanning-tree bpdu-guard	Shuts down an edge port if it receives a BPDU	IC
spanning-tree cost	Configures the spanning tree path cost of an interface	IC
spanning-tree edge-port	Enables fast forwarding for edge ports	IC
spanning-tree link-type	Configures the link type for RSTP/MSTP	IC
spanning-tree loopback-detection	Enables BPDU loopback detection for a port	IC
spanning-tree loopback-detection release-mode	Configures loopback release mode for a port	IC

Table 102: Spanning Tree Commands (Continued)

Command	Function	Mode
spanning-tree loopback-detection trap	Enables BPDU loopback SNMP trap notification for a port	IC
spanning-tree mst cost	Configures the path cost of an instance in the MST	IC
spanning-tree mst port-priority	Configures the priority of an instance in the MST	IC
spanning-tree portfast	Sets an interface to fast forwarding	IC
spanning-tree port-bpdu-flooding	Floods BPDUs to other ports when global spanning tree is disabled	IC
spanning-tree port-priority	Configures the spanning tree priority of an interface	IC
spanning-tree root-guard	Prevents a designated port from passing superior BPDUs	IC
spanning-tree spanning-disabled	Disables spanning tree for an interface	IC
spanning-tree loopback-detection release	Manually releases a port placed in discarding state by loopback-detection	PE
spanning-tree protocol-migration	Re-checks the appropriate BPDU format	PE
show spanning-tree	Shows spanning tree configuration for the common spanning tree (i.e., overall bridge), a selected interface, or an instance within the multiple spanning tree	PE
show spanning-tree mst configuration	Shows the multiple spanning tree configuration	PE

spanning-tree

This command enables the Spanning Tree Algorithm globally for the switch. Use the **no** form to disable it.

SYNTAX

[**no**] **spanning-tree**

DEFAULT SETTING

Spanning tree is enabled.

COMMAND MODE

Global Configuration

COMMAND USAGE

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

EXAMPLE

This example shows how to enable the Spanning Tree Algorithm for the switch:

```
Console(config)#spanning-tree
Console(config)#
```

spanning-tree cisco-prestandard

This command configures spanning tree operation to be compatible with Cisco prestandard versions. Use the **no** form to restore the default setting.

[**no**] **spanning-tree cisco-prestandard**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

Cisco prestandard versions prior to Cisco IOS Release 12.2(25)SEC do not fully follow the IEEE standard, causing some state machine procedures to function incorrectly. The command forces the spanning tree protocol to function in a manner compatible with Cisco prestandard versions.

EXAMPLE

```
Console(config)#spanning-tree cisco-prestandard
Console(config)#
```

spanning-tree forward-time

This command configures the spanning tree bridge forward time globally for this switch. Use the **no** form to restore the default setting.

SYNTAX

spanning-tree forward-time *seconds*

no spanning-tree forward-time

seconds - Time in seconds. (Range: 4 - 30 seconds)
The minimum value is the higher of 4 or [(max-age / 2) + 1].

DEFAULT SETTING

15 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

This command sets the maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to the discarding state; otherwise, temporary data loops might result.

EXAMPLE

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

spanning-tree hello-time

This command configures the spanning tree bridge hello time globally for this switch. Use the **no** form to restore the default.

SYNTAX

spanning-tree hello-time *time*

no spanning-tree hello-time

time - Time in seconds. (Range: 1-10 seconds).
The maximum value is the lower of 10 or [(max-age / 2) - 1].

DEFAULT SETTING

2 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

This command sets the time interval (in seconds) at which the root device transmits a configuration message.

EXAMPLE

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

RELATED COMMANDS

spanning-tree forward-time (745)
spanning-tree max-age (747)

spanning-tree max-age

This command configures the spanning tree bridge maximum age globally for this switch. Use the **no** form to restore the default.

SYNTAX

spanning-tree max-age *seconds*

no spanning-tree max-age

seconds - Time in seconds. (Range: 6-40 seconds)
The minimum value is the higher of 6 or [2 x (hello-time + 1)].
The maximum value is the lower of 40 or [2 x (forward-time - 1)].

DEFAULT SETTING

20 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

This command sets the maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

EXAMPLE

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

RELATED COMMANDS

spanning-tree forward-time (745)
spanning-tree hello-time (746)

spanning-tree mode

This command selects the spanning tree mode for this switch. Use the **no** form to restore the default.

SYNTAX

spanning-tree mode {**stp** | **rstp** | **mstp**}

no spanning-tree mode

stp - Spanning Tree Protocol (IEEE 802.1D)

rstp - Rapid Spanning Tree Protocol (IEEE 802.1w)

mstp - Multiple Spanning Tree (IEEE 802.1s)

DEFAULT SETTING

rstp

COMMAND MODE
Global Configuration

COMMAND USAGE
- Spanning Tree Protocol
  Uses RSTP for the internal state machine, but sends only 802.1D BPDUs. This creates one spanning tree instance for the entire network. If multiple VLANs are implemented on a network, the path between specific VLAN members may be inadvertently disabled to prevent network loops, thus isolating group members. When operating multiple VLANs, we recommend selecting the MSTP option.

- Rapid Spanning Tree Protocol
  RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:

  - STP Mode – If the switch receives an 802.1D BPDU after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.

  - RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

- Multiple Spanning Tree Protocol

  - To allow multiple spanning trees to operate over the network, you must configure a related set of bridges with the same MSTP configuration, allowing them to participate in a specific set of spanning tree instances.

  - A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments.

  - Be careful when switching between spanning tree modes. Changing modes stops all spanning-tree instances for the previous mode and restarts the system in the new mode, temporarily disrupting user traffic.

EXAMPLE
The following example configures the switch to use Rapid Spanning Tree:

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

spanning-tree pathcost method

This command configures the path cost method used for Rapid Spanning Tree and Multiple Spanning Tree. Use the **no** form to restore the default.

SYNTAX

spanning-tree pathcost method {**long** | **short**}

no spanning-tree pathcost method

long - Specifies 32-bit based values that range from 1-200,000,000. This method is based on the IEEE 802.1w Rapid Spanning Tree Protocol.

short - Specifies 16-bit based values that range from 1-65535. This method is based on the IEEE 802.1 Spanning Tree Protocol.

DEFAULT SETTING

Long method

COMMAND MODE

Global Configuration

COMMAND USAGE

- The path cost method is used to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Note that path cost (page 757) takes precedence over port priority (page 765).
- The path cost methods apply to all spanning tree modes (STP, RSTP and MSTP). Specifically, the long method can be applied to STP since this mode is supported by a backward compatible mode of RSTP.

EXAMPLE

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

spanning-tree priority

This command configures the spanning tree priority globally for this switch. Use the **no** form to restore the default.

SYNTAX

spanning-tree priority *priority*

no spanning-tree priority

priority - Priority of the bridge. (Range – 0-61440, in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

DEFAULT SETTING

32768

COMMAND MODE
Global Configuration

COMMAND USAGE
Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority (i.e., lower numeric value) becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

EXAMPLE

```
Console(config)#spanning-tree priority 40000
Console(config)#
```

spanning-tree mst configuration

This command changes to Multiple Spanning Tree (MST) configuration mode.

DEFAULT SETTING
No VLANs are mapped to any MST instance.
The region name is set the switch's MAC address.

COMMAND MODE
Global Configuration

EXAMPLE

```
Console(config)#spanning-tree mst configuration
Console(config-mstp)#
```

RELATED COMMANDS
mst vlan (753)
mst priority (752)
name (754)
revision (754)
max-hops (752)

spanning-tree system-bpdu-flooding

This command configures the system to flood BPDUs to all other ports on the switch or just to all other ports in the same VLAN when spanning tree is disabled globally on the switch or disabled on a specific port. Use the **no** form to restore the default.

SYNTAX

spanning-tree system-bpdu-flooding {**to-all** | **to-vlan**}

no spanning-tree system-bpdu-flooding

to-all - Floods BPDUs to all other ports on the switch.

to-vlan - Floods BPDUs to all other ports within the receiving port's native VLAN (i.e., as determined by port's PVID).

DEFAULT SETTING

Floods to all other ports in the same VLAN.

COMMAND MODE

Global Configuration

COMMAND USAGE

The **spanning-tree system-bpdu-flooding** command has no effect if BPDU flooding is disabled on a port (see the spanning-tree port-bpdu-flooding command).

EXAMPLE

```
Console(config)#spanning-tree system-bpdu-flooding
Console(config)#
```

spanning-tree transmission-limit

This command configures the minimum interval between the transmission of consecutive BPDUs. Use the **no** form to restore the default.

SYNTAX

spanning-tree transmission-limit *count*

no spanning-tree transmission-limit

count - The transmission limit in seconds. (Range: 1-10)

DEFAULT SETTING

3

COMMAND MODE

Global Configuration

COMMAND USAGE

This command limits the maximum transmission rate for BPDUs.

EXAMPLE

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

max-hops

This command configures the maximum number of hops in the region before a BPDU is discarded. Use the **no** form to restore the default.

SYNTAX

max-hops *hop-number*

hop-number - Maximum hop number for multiple spanning tree. (Range: 1-40)

DEFAULT SETTING

20

COMMAND MODE

MST Configuration

COMMAND USAGE

An MSTI region is treated as a single node by the STP and RSTP protocols. Therefore, the message age for BPDUs inside an MSTI region is never changed. However, each spanning tree instance within a region, and the internal spanning tree (IST) that connects these instances use a hop count to specify the maximum number of bridges that will propagate a BPDU. Each bridge decrements the hop count by one before passing on the BPDU. When the hop count reaches zero, the message is dropped.

EXAMPLE

```
Console(config-mstp)#max-hops 30
Console(config-mstp)#
```

mst priority

This command configures the priority of a spanning tree instance. Use the **no** form to restore the default.

SYNTAX

mst *instance-id* **priority** *priority*

no mst *instance-id* **priority**

instance-id - Instance identifier of the spanning tree. (Range: 0-4094)

priority - Priority of the a spanning tree instance. (Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

DEFAULT SETTING
32768

COMMAND MODE
MST Configuration

COMMAND USAGE
- MST priority is used in selecting the root bridge and alternate bridge of the specified instance. The device with the highest priority (i.e., lowest numerical value) becomes the MSTI root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

- You can set this switch to act as the MSTI root device by specifying a priority of 0, or as the MSTI alternate device by specifying a priority of 16384.

EXAMPLE

```
Console(config-mstp)#mst 1 priority 4096
Console(config-mstp)#
```

mst vlan

This command adds VLANs to a spanning tree instance. Use the **no** form to remove the specified VLANs. Using the **no** form without any VLAN parameters to remove all VLANs.

SYNTAX

[**no**] **mst** *instance-id* **vlan** *vlan-range*

instance-id - Instance identifier of the spanning tree. (Range: 0-4094)

vlan-range - Range of VLANs. (Range: 1-4094)

DEFAULT SETTING
none

COMMAND MODE
MST Configuration

COMMAND USAGE
- Use this command to group VLANs into spanning tree instances. MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.

- By default all VLANs are assigned to the Internal Spanning Tree (MSTI 0) that connects all bridges and LANs within the MST region. This switch supports up to 58 instances. You should try to group VLANs

which cover the same general area of your network. However, remember that you must configure all bridges within the same MSTI Region (page 754) with the same set of instances, and the same instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each MSTI region as a single node, connecting all regions to the Common Spanning Tree.

EXAMPLE

```
Console(config-mstp)#mst 1 vlan 2-5
Console(config-mstp)#
```

name

This command configures the name for the multiple spanning tree region in which this switch is located. Use the **no** form to clear the name.

SYNTAX

name *name*

name - Name of the spanning tree.

DEFAULT SETTING

Switch's MAC address

COMMAND MODE

MST Configuration

COMMAND USAGE

The MST region name and revision number (page 754) are used to designate a unique MST region. A bridge (i.e., spanning-tree compliant device such as this switch) can only belong to one MST region. And all bridges in the same region must be configured with the same MST instances.

EXAMPLE

```
Console(config-mstp)#name R&D
Console(config-mstp)#
```

RELATED COMMANDS

revision (754)

revision

This command configures the revision number for this multiple spanning tree configuration of this switch. Use the **no** form to restore the default.

SYNTAX

revision *number*

number - Revision number of the spanning tree. (Range: 0-65535)

DEFAULT SETTING
0

COMMAND MODE
MST Configuration

COMMAND USAGE
The MST region name (page 754) and revision number are used to designate a unique MST region. A bridge (i.e., spanning-tree compliant device such as this switch) can only belong to one MST region. And all bridges in the same region must be configured with the same MST instances.

EXAMPLE

```
Console(config-mstp)#revision 1
Console(config-mstp)#
```

RELATED COMMANDS
name (754)

spanning-tree bpdu-filter

This command filters all BPDUs received on an edge port. Use the **no** form to disable this feature.

SYNTAX

[**no**] **spanning-tree bpdu-filter**

DEFAULT SETTING
Disabled

COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE
- This command filters all Bridge Protocol Data Units (BPDUs) received on an interface to save CPU processing time. This function is designed to work in conjunction with edge ports which should only connect end stations to the switch, and therefore do not need to process BPDUs. However, note that if a trunking port connected to another switch or bridging device is mistakenly configured as an edge port, and BPDU filtering is enabled on this port, this might cause a loop in the spanning tree.

- Before enabling BPDU Filter, the interface must first be configured as an edge port with the spanning-tree edge-port or spanning-tree portfast command.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree bpdu-filter
Console(config-if)#
```

RELATED COMMANDS

spanning-tree edge-port (758)
spanning-tree portfast (764)

spanning-tree bpdu-guard

This command shuts down an edge port (i.e., an interface set for fast forwarding) if it receives a BPDU. Use the **no** form to disable this feature.

SYNTAX

[**no**] **spanning-tree bpdu-guard**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- An edge port should only be connected to end nodes which do not generate BPDUs. If a BPDU is received on an edge port, this indicates an invalid network configuration, or that the switch may be under attack by a hacker. If an interface is shut down by BPDU Guard, it must be manually re-enabled using the no spanning-tree spanning-disabled command.

- Before enabling BPDU Guard, the interface must be configured as an edge port with the spanning-tree edge-port or spanning-tree portfast command. Also note that if the edge port attribute is disabled on an interface, BPDU Guard will also be disabled on that interface.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree bpdu-guard
Console(config-if)#
```

RELATED COMMANDS

spanning-tree edge-port (758)
spanning-tree spanning-disabled (767)

spanning-tree cost

This command configures the spanning tree path cost for the specified interface. Use the **no** form to restore the default auto-configuration mode.

SYNTAX

spanning-tree cost *cost*

no spanning-tree cost

cost - The path cost for the port. (Range: 0 for auto-configuration, 1-65535 for short path cost method[20], 1-200,000,000 for long path cost method)

Table 103: Recommended STA Path Cost Range

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

Table 104: Recommended STA Path Cost

Port Type	Link Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex	100	2,000,000
	Full Duplex	95	1,999,999
	Trunk	90	1,000,000
Fast Ethernet	Half Duplex	19	200,000
	Full Duplex	18	100,000
	Trunk	15	50,000
Gigabit Ethernet	Full Duplex	4	10,000
	Trunk	3	5,000

DEFAULT SETTING

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

Table 105: Default STA Path Costs

Port Type	Link Type	IEEE 802.1w-2001
Ethernet	Half Duplex	2,000,000
	Full Duplex	1,000,000
	Trunk	500,000
Fast Ethernet	Half Duplex	200,000
	Full Duplex	100,000
	Trunk	50,000
Gigabit Ethernet	Full Duplex	10,000
	Trunk	5,000

20. Use the spanning-tree pathcost method command to set the path cost method.

COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE
- This command is used by the Spanning Tree Algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.
- Path cost takes precedence over port priority.
- When the path cost method (page 749) is set to short, the maximum value for path cost is 65,535.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

spanning-tree edge-port

This command specifies an interface as an edge port. Use the **no** form to restore the default.

SYNTAX

spanning-tree edge-port [**auto**]

no spanning-tree edge-port

auto - Automatically determines if an interface is an edge port.

DEFAULT SETTING
Disabled

COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE
- You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related time out problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.
- This command has the same effect as the spanning-tree portfast.

- If the "auto" option is used, the port will be automatically configured as an edge port if the port state has transitioned from discarding to forwarding, and the edge delay time expires without receiving any RSTP or MSTP BPDUs. Note that edge delay time (802.1D-2004 17.20.4) equals the protocol migration time if a port's link type is point-to-point; otherwise it equals the spanning-tree's maximum age (page 747).

  An interface cannot function as an edge port under the following conditions:

  - If spanning tree mode is set to STP (page 747), edge-port mode can be manually enabled or set to auto, but will have no effect.
  - If loopback detection is enabled (page 760) and a loopback BPDU is detected, the interface cannot function as an edge port until the loopback state is released (page 760).
  - If an interface is in forwarding state and its role changes, the interface cannot continue to function as an edge port even if the edge delay time has expired.

    If the port does not receive any BPDUs after the edge delay timer expires, its role changes to designated port and it immediately enters forwarding state (see "Displaying Interface Settings for STA").

    The edge delay time equals the protocol migration time when the port link type is point-to-point (which is 3 seconds as defined in IEEE 802.3D-2004 17.20.4), otherwise it equals the maximum age for configuration messages (see the spanning-tree max-age command).

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

spanning-tree link-type

This command configures the link type for Rapid Spanning Tree and Multiple Spanning Tree. Use the **no** form to restore the default.

SYNTAX

spanning-tree link-type {**auto** | **point-to-point** | **shared**}

no spanning-tree link-type

auto - Automatically derived from the duplex mode setting.

point-to-point - Point-to-point link.

shared - Shared medium.

DEFAULT SETTING

auto

COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE
- Specify a point-to-point link if the interface can only be connected to exactly one other bridge, or a shared link if it can be connected to two or more bridges.
- When automatic detection is selected, the switch derives the link type from the duplex mode. A full-duplex interface is considered a point-to-point link, while a half-duplex interface is assumed to be on a shared link.
- RSTP only works on point-to-point links between two bridges. If you designate a port as a shared link, RSTP is forbidden. Since MSTP is an extension of RSTP, this same restriction applies.

EXAMPLE
```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree link-type point-to-point
```

spanning-tree loopback-detection

This command enables the detection and response to Spanning Tree loopback BPDU packets on the port. Use the **no** form to disable this feature.

SYNTAX
[**no**] **spanning-tree loopback-detection**

DEFAULT SETTING
Enabled

COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE
- If Port Loopback Detection is not enabled and a port receives it's own BPDU, then the port will drop the loopback BPDU according to IEEE Standard 802.1W-2001 9.3.4 (Note 1).
- Port Loopback Detection will not be active if Spanning Tree is disabled on the switch.

EXAMPLE
```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection
```

spanning-tree loopback-detection release-mode

This command configures the release mode for a port that was placed in the discarding state because a loopback BPDU was received. Use the **no** form to restore the default.

SYNTAX

spanning-tree loopback-detection release-mode
{**auto** | **manual**}

no spanning-tree loopback-detection release-mode

auto - Allows a port to automatically be released from the discarding state when the loopback state ends.

manual - The port can only be released from the discarding state manually.

DEFAULT SETTING

auto

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- If the port is configured for automatic loopback release, then the port will only be returned to the forwarding state if one of the following conditions is satisfied:
  - The port receives any other BPDU except for it's own, or;
  - The port's link status changes to link down and then link up again, or;
  - The port ceases to receive it's own BPDUs in a forward delay interval.
- If Port Loopback Detection is not enabled and a port receives it's own BPDU, then the port will drop the loopback BPDU according to IEEE Standard 802.1W-2001 9.3.4 (Note 1).
- Port Loopback Detection will not be active if Spanning Tree is disabled on the switch.
- When configured for manual release mode, then a link down / up event will not release the port from the discarding state.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection release-mode manual
```

spanning-tree loopback-detection trap

This command enables SNMP trap notification for Spanning Tree loopback BPDU detections. Use the **no** form to restore the default.

SYNTAX

[**no**] **spanning-tree loopback-detection trap**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection trap
```

spanning-tree mst cost

This command configures the path cost on a spanning instance in the Multiple Spanning Tree. Use the **no** form to restore the default auto-configuration mode.

SYNTAX

spanning-tree mst *instance-id* **cost** *cost*

no spanning-tree mst *instance-id* **cost**

instance-id - Instance identifier of the spanning tree. (Range: 0-4094, no leading zeroes)

cost - Path cost for an interface. (Range: 0 for auto-configuration, 1-65535 for short path cost method[21], 1-200,000,000 for long path cost method)

The recommended path cost range is listed in Table 103. The recommended path cost is listed in Table 104.

DEFAULT SETTING

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the defaults listed in Table 105. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- Each spanning-tree instance is associated with a unique set of VLANs.

21. Use the spanning-tree pathcost method command to set the path cost method.

- This command is used by the multiple spanning-tree algorithm to determine the best path between devices. Therefore, lower values should be assigned to interfaces attached to faster media, and higher values assigned to interfaces with slower media.
- Use the **no spanning-tree mst cost** command to specify auto-configuration mode.
- Path cost takes precedence over interface priority.

EXAMPLE

```
Console(config)#interface Ethernet 1/5
Console(config-if)#spanning-tree mst 1 cost 50
Console(config-if)#
```

RELATED COMMANDS

spanning-tree mst port-priority (763)

spanning-tree mst port-priority

This command configures the interface priority on a spanning instance in the Multiple Spanning Tree. Use the **no** form to restore the default.

SYNTAX

spanning-tree mst *instance-id* **port-priority** *priority*

no spanning-tree mst *instance-id* port-priority

instance-id - Instance identifier of the spanning tree. (Range: 0-4094, no leading zeroes)

priority - Priority for an interface. (Range: 0-240 in steps of 16)

DEFAULT SETTING

128

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- This command defines the priority for the use of an interface in the multiple spanning-tree. If the path cost for all interfaces on a switch are the same, the interface with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- Where more than one interface is assigned the highest priority, the interface with lowest numeric identifier will be enabled.

EXAMPLE

```
Console(config)#interface Ethernet 1/5
Console(config-if)#spanning-tree mst 1 port-priority 0
Console(config-if)#
```

RELATED COMMANDS
spanning-tree mst cost (762)

spanning-tree portfast

This command sets an interface to fast forwarding. Use the **no** form to disable fast forwarding.

SYNTAX

[**no**] **spanning-tree portfast**

DEFAULT SETTING
Disabled

COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE
- This command is used to enable/disable the fast spanning-tree mode for the selected port. In this mode, ports skip the Discarding and Learning states, and proceed straight to Forwarding.
- Since end-nodes cannot cause forwarding loops, they can be passed through the spanning tree state changes more quickly than allowed by standard convergence time. Fast forwarding can achieve quicker convergence for end-node workstations and servers, and also overcome other STA related timeout problems. (Remember that fast forwarding should only be enabled for ports connected to a LAN segment that is at the end of a bridged LAN or for an end-node device.)
- This command is the same as spanning-tree edge-port, and is only included for backward compatibility with earlier products. Note that this command may be removed for future software versions.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#bridge-group 1 portfast
Console(config-if)#
```

RELATED COMMANDS
spanning-tree edge-port (758)

spanning-tree port-bpdu-flooding

This command floods BPDUs to other ports when spanning tree is disabled globally or disabled on a specific port. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **spanning-tree port-bpdu-flooding**

DEFAULT SETTING
Enabled

COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE
- When enabled, BPDUs are flooded to all other ports on the switch or to all other ports within the receiving port's native VLAN as specified by the spanning-tree system-bpdu-flooding command.
- The spanning-tree system-bpdu-flooding command has no effect if BPDU flooding is disabled on a port by the **spanning-tree port-bpdu-flooding** command.

EXAMPLE
```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-bpdu-flooding
Console(config-if)#
```

spanning-tree port-priority

This command configures the priority for the specified interface. Use the **no** form to restore the default.

SYNTAX
spanning-tree port-priority *priority*

no spanning-tree port-priority

priority - The priority for a port. (Range: 0-240, in steps of 16)

DEFAULT SETTING
128

COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE
- This command defines the priority for the use of a port in the Spanning Tree Algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

EXAMPLE
```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 0
```

RELATED COMMANDS
spanning-tree cost (757)

spanning-tree root-guard

This command prevents a designated port[22] from taking superior BPDUs into account and allowing a new STP root port to be elected. Use the **no** form to disable this feature.

SYNTAX

[**no**] **spanning-tree root-guard**

DEFAULT SETTING
Disabled

COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE
- A bridge with a lower bridge identifier (or same identifier and lower MAC address) can take over as the root bridge at any time.
- When Root Guard is enabled, and the switch receives a superior BPDU on this port, it is set to the Discarding state until it stops receiving superior BPDUs for a fixed recovery period. While in the discarding state, no traffic is forwarded across the port.
- Root Guard can be used to ensure that the root bridge is not formed at a suboptimal location. Root Guard should be enabled on any designated port connected to low-speed bridges which could potentially overload a slower link by taking over as the root port and forming a new spanning tree topology. It could also be used to form a border around part of the network where the root bridge is allowed.
- When spanning tree is initialized globally on the switch or on an interface, the switch will wait for 20 seconds to ensure that the spanning tree has converged before enabling Root Guard.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree root-guard
Console(config-if)#
```

22. See Port Role under "Displaying Interface Settings for STA."

spanning-tree spanning-disabled

This command disables the spanning tree algorithm for the specified interface. Use the **no** form to re-enable the spanning tree algorithm for the specified interface.

SYNTAX

[**no**] **spanning-tree spanning-disabled**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

EXAMPLE

This example disables the spanning tree algorithm for port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree spanning-disabled
Console(config-if)#
```

spanning-tree loopback-detection release

This command manually releases a port placed in discarding state by loopback-detection.

SYNTAX

spanning-tree loopback-detection release *interface*

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

COMMAND USAGE

Use this command to release an interface from discarding state if loopback detection release mode is set to "manual" by the spanning-tree loopback-detection release-mode command and BPDU loopback occurs.

EXAMPLE

```
Console#spanning-tree loopback-detection release ethernet 1/1
Console#
```

spanning-tree protocol-migration

This command re-checks the appropriate BPDU format to send on the selected interface.

SYNTAX

spanning-tree protocol-migration *interface*

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

COMMAND USAGE

If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the **spanning-tree protocol-migration** command at any time to manually re-check the appropriate BPDU format to send on the selected interfaces (i.e., RSTP or STP-compatible).

EXAMPLE

```
Console#spanning-tree protocol-migration eth 1/5
Console#
```

show spanning-tree

This command shows the configuration for the common spanning tree (CST) or for an instance within the multiple spanning tree (MST).

SYNTAX

show spanning-tree [*interface* | **mst** *instance-id* | **stp-enabled-only**]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

instance-id - Instance identifier of the multiple spanning tree. (Range: 0-4094, no leading zeroes)

stp-enabled-only - Displays global settings, and settings for interfaces for which STP is enabled.

DEFAULT SETTING

None

COMMAND MODE
Privileged Exec

COMMAND USAGE
- Use the **show spanning-tree** command with no parameters to display the spanning tree configuration for the switch for the Common Spanning Tree (CST) and for every interface in the tree.
- Use the **show spanning-tree** *interface* command to display the spanning tree configuration for an interface within the Common Spanning Tree (CST).
- Use the **show spanning-tree mst** *instance-id* command to display the spanning tree configuration for an instance within the Multiple Spanning Tree (MST).
- For a description of the items displayed under "Spanning-tree information," see "Configuring Global Settings for STA." For a description of the items displayed for specific interfaces, see "Displaying Interface Settings for STA."

EXAMPLE

```
Console#show spanning-tree
Spanning Tree Information
---------------------------------------------------------------
 Spanning Tree Mode:               MSTP
 Spanning Tree Enabled/Disabled:   Enabled
 Instance:                         0
 VLANs Configuration:              1-4094
 Priority:                         32768
 Bridge Hello Time (sec.):         2
 Bridge Max Age (sec.):            20
 Bridge Forward Delay (sec.):      15
 Root Hello Time (sec.):           2
 Root Max Age (sec.):              20
 Root Forward Delay (sec.):        15
 Max Hops:                         20
 Remaining Hops:                   20
 Designated Root:                  32768.0.0001ECF8D8C6
 Current Root Port:                1
 Current Root Cost:                100000
 Number of Topology Changes:       3
 Last Topology Change Time (sec.): 14142
 Transmission Limit:               3
 Path Cost Method:                 Long
 Flooding Behavior:                To VLAN
 Cisco Prestandard:                Disabled
---------------------------------------------------------------
Eth  1/ 1 information
---------------------------------------------------------------
 Admin Status:                     Enabled
 Role:                             Root
 State:                            Forwarding
 External Admin Path Cost:         0
 Internal Admin Path Cost:         0
 External Oper Path Cost:          100000
 Internal Oper Path Cost:          100000
 Priority:                         128
 Designated Cost:                  0
```

```
 Designated Port:                  128.14
 Designated Root:                  32768.0.0001ECF8D8C6
 Designated Bridge:                32768.0.0001ECF8D8C6
 Fast Forwarding:                  Enabled
 Forward Transitions:              1
 Last Topology Change Time (sec.): 14210
 Admin Edge Port:                  Enabled
 Oper Edge Port:                   Disabled
 Admin Link Type:                  Auto
 Oper Link Type:                   Point-to-point
 Flooding Behavior:                Enabled
 Spanning Tree Status:             Enabled
 Loopback Detection Status:        Enabled
 Loopback Detection Release Mode:  Auto
 Loopback Detection Trap:          Disabled
 Loopback Detection Action:        Block
 Admin Root Guard:                 Disabled
 Oper Root Guard:                  Disabled
 BPDU Guard:                       Disabled
 BPDU Filtering:                   Disabled
.
.
.
```

show spanning-tree mst configuration

This command shows the configuration of the multiple spanning tree.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show spanning-tree mst configuration
Mstp Configuration Information
-----------------------------------------------------------------
 Configuration Name : R&D
 Revision Level     :0

 Instance VLANs
-----------------------------------------------------------------
     0    1-4094
Console#
```

35 EAPS COMMANDS

NOTE: The information provided in this section is based on RFC 3619.

Ethernet Automatic Protection Switching™ (EAPS) can be used to increase the availability and robustness of Ethernet rings. An Ethernet ring built using EAPS can have resilience comparable to that provided by SONET BSHR or SDH MS-SPRing configurations, at a lower cost and with fewer constraints (for example, ring size).

Many Metropolitan Area Networks (MANs) use a ring topology. EAPS works well in ring topologies for either MANs or LANs. MAN operators want to minimize the recovery time in the event of a fiber cut. EAPS technology converges in less than one second, often in less than 500 milliseconds. Also, EAPS does not limit the number of nodes in the ring, and the convergence time is independent of the number of nodes in the ring.

Operational Concept – An EAPS Domain exists on a single Ethernet ring. Any VLAN that is to be protected is configured on all ports in the ring for the given EAPS Domain. Each EAPS Domain has a single designated "master node." All other nodes on that ring are referred to as "transit nodes."

Each node has two ports connected to the ring. One port of the master node is designated as the "primary port" to the ring, carrying control messages and data, while the other port is designated as the "secondary port" and runs in backup mode.

In normal operation, the master node blocks the secondary port for all non-control Ethernet frames belonging to the given EAPS Domain, thereby avoiding a loop in the ring. Existing Ethernet switching and learning mechanisms operate per existing standards on this ring. This is possible because the master node makes the ring appear as though there is no loop from the perspective of the Ethernet standard algorithms used for switching and learning. If the master node detects a ring fault, it unblocks its secondary port and allows Ethernet data frames to pass through that port. There is also a special "Control VLAN" that can always pass through all ports in the EAPS Domain, including the secondary port of the master node.

EAPS uses both a polling mechanism and an alert mechanism, described below, to verify the connectivity of the ring and quickly detect any faults.

Link Down Alert – When a transit node detects a link-down on any of its ports in the EAPS Domain, that transit node immediately sends a "link down" control frame on the Control VLAN to the master node.

When the master node receives this "link down" control frame, the master node moves from the "normal" state to the ring-fault state and unblocks its secondary port. The master node also flushes its bridging table, and sends a control frame to all other ring nodes, instructing them to flush their bridging tables as well. Immediately after flushing its bridging table, each node begins learning the new topology.

Ring Polling – The master node sends a health-check frame on the Control VLAN at a user-configurable interval. If the ring is complete, the health-check frame will be received on its secondary port, and the master node resets its fail-period timer and continues normal operation.

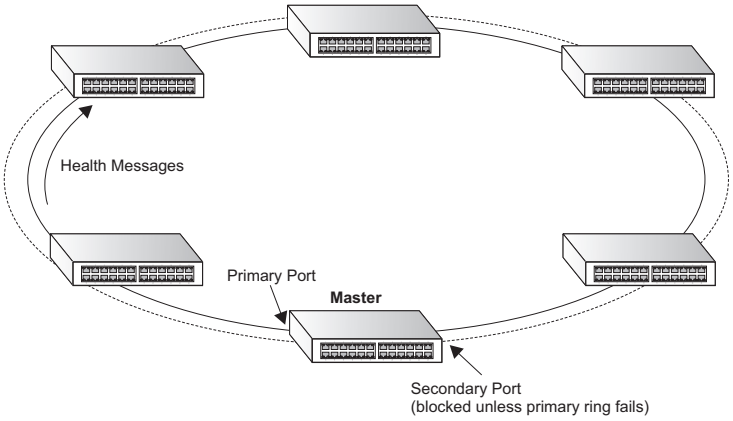
If the master node does not receive the health-check frame before the fail-period timer expires, the master node moves from normal state to "ring-fault" state and unblocks its secondary port. The master node flushes its bridging table and sends a control frame to all other nodes, instructing them to also flush their bridging tables. Immediately after flushing its bridge table, each node starts learning the new topology. This ring polling mechanism provides a backup in the event that the Link Down Alert frame should get lost for some unforeseen reason.

Ring Restoration – The master node continues sending periodic health-check frames out its primary port even when operating in the ring-fault state. Once the ring is restored, the next health-check frame will be received on the master node's secondary port. This will cause the master node to transition back to the normal state, logically block non-control frames on the secondary port, flush its own bridge table, and send a control frame to the transit nodes, instructing them to flush their bridging tables and re-learn the topology.

During the time between the transit node detecting that its link is restored and the master node detecting that the ring is restored, the secondary port of the master node is still open °V creating the possibility of a temporary loop in the topology. To prevent this, the transit node will place all the protected VLANs transiting the newly restored port into a temporary blocked state, remember which port has been temporarily blocked, and then transition into the "pre-forwarding" state. When the transit node in the "pre-forwarding" state receives a control frame instructing it to flush its bridging table, it will flush the bridging table, unblock the previously blocked protected VLANs on the newly restored port, and transition to the "normal" state.

Multiple EAPS Domains – An EAPS-enabled switch can be part of more than one ring. Hence, an EAPS-enabled switch can belong to more than one EAPS Domain at the same time. Each EAPS Domain on an switch requires a separate instance of the EAPS protocol on that same switch, one instance per EAPS-protected ring.

There can also be more than one EAPS domain running on the same ring at the same time. Each EAPS Domain has its own unique master node and its own set of protected VLANs. This facilitates reuse of the ring's bandwidth.



Functional Description

- Setting port status on the master node: When the master node is in the Complete state, the primary and secondary ports will be set to the status described below. On the CVLAN, the secondary port will trap control messages to the CPU and not forward them to any port. On Protected VLANs, the secondary port will block all data flow except for EAPS domain control messages.

- Setting port status on the transit node: The port on the domain ring will periodically receive a control message. This message is copied to the CPU and forwarded to the next port on the domain ring. When the port on the domain ring link changes from up to down, this port will be temporarily blocked on the Protected VLANs. This port is opened on the Protected VLANs again only when the transit node in "pre-forwarding" state receives a control frame instructing it to flush its bridging table and unblock the previously blocked protected VLANs.

- Handling a hardware link down event: If this event occurs on the primary port of the master node, the master node will unblock the blocked port on the Protected VLAN and send a message to flush the forwarding database (FDB) to all transit nodes. If this event occurs on the secondary port, the master node will enter failed state. If this event occurs on a transit node, the transit node will send a link down control message to the master node, and the master node will unblock the blocked port and send a control message to make the transit nodes flush their FDB. The master node also enters the failed state.

- Handling a hardware link up event: If this event occurs on the master node, the secondary port will be blocked on the Protected VLAN, and the master node will send a message to flush the FDB to all transit nodes. If this event occurs on a transit node, the new linked port will be blocked until it receives RING-UP-FLUSH-FDB message.

- Handling health-check packet hello timer events: The master node sends a health-check packet to ensure the ring status, and starts the health-check packet fail timer at once.

- Handling health-check packet fail timer events: If this event occurs, the ring topology has changed, and the link down control message lost. The

master node enters failed state and sends a control message to make all transit nodes flush their FDB.

- Handling EAPS control message events: Control messages are sent to nodes on the domain ring to maintain ring status. The master node sends health-check packets to ensure that the domain ring is unchanged. The master node sends RING-DOWN-FLUSH-FDB and RING-UP-FLUSH-FDB messages to inform the transit nodes to flush their FDB. Transit nodes sends a link-down message to the master node to make master enter failed state immediately.

NOTE: The port MAC address, not the system MAC address, is used as the source address for all EAPS protocol packets.

Configuration Limitations for EAPS

The following configuration limitations apply to EAPS:

- One switch only supports two EAPS domains – each domain must have one control VLAN and at most 10 Protected VLANs.
- Gigabit Ethernet ports can be configured as EAPS ring ports, but these ports should not be a member of any trunk.
- Each EAPS domain can have only one master node.
- The hello timer and fail timer must be configured on the master node. Afterwards, the master node will send timer configuration messages to the transit nodes to reset their hello-timer and fail-timer.
- One VLAN must be added to an EAPS domain as the CVLAN. This can be designated as any VLAN, other than the management VLAN. The CVLAN should only contain ring ports, and must NOT be configured with an IP address.

This section describes commands used to configure EAPS.

Table 106: EAPS Commands

Command	Function	Mode
eaps	Enables EAPS globally on the switch	GC
eaps domain	Creates an EAPS domain	GC
control-vlan	Adds a Control VLAN to an EAPS domain	EAPS
enable	Activates an EAPS domain	EAPS
failtime	Sets the time to wait for a health-check packet	EAPS
hellotime	Sets the interval at which to send health-check packets	EAPS
mode	Configures master node or transit node	EAPS
port	Sets port type on a ring as primary or secondary	EAPS

Table 106: EAPS Commands(Continued)

Command	Function	Mode
protect-vlan	Adds a Protected VLAN to an EAPS domain	EAPS
show eaps	Displays status information for configured EAPS domains	PE

Configuration Guidelines for EAPS

1. Create or delete an EAPS domain: Create or delete a domain using the eaps domain command. The domain name is used as the index for this domain in the EAPS database. To delete an EAPS Domain, use the no enable command to disable the domain, followed by the no eaps domain command to delete the specified domain. If a port on the domain ring has not been added to another domain ring, this port will be reset to operate as a normal port. The database of this domain will then be cleared.

2. Define the EAPS mode of the switch: After creating an EAPS domain, define the EAPS mode for this node using the mode command. Only one node can be defined as the master node on a domain ring, all the other ports should be defined as transit nodes.

3. Configure EAPS polling timers: Set the values of the polling timers the master node uses for the EAPS health-check packet that is circulated around the ring for an EAPS domain using the hellotime and failtime commands. The hello-timer is the periodic time at which the master sends a health-check packet, and the fail-time is the time the master waits to receive back a health-check packet from the other direction in the ring.

4. Configure the primary and secondary ports: Each node on the ring connects to it through two ring ports. Use the port primary command (page 781) to configure one port as the primary port; and the port secondary command to configure the other as the secondary port.

5. Configure the EAPS Control VLAN (CVLAN): Use the control-vlan command to create the VLAN used to pass ring integrity commands. The CVLAN is automatically assigned a QoS profile of Qp8 (with the QoS High priority setting). The CVLAN must NOT be configured with an IP address. In addition, only ring ports may be added to the CVLAN (prior to configuring the VLAN as a CVLAN). No other ports can be members of this VLAN (once set as a CVLAN). Also, the ring ports of the CVLAN must be tagged. Failure to observe these restrictions can result in a loop in the network.

6. Configuring EAPS Protected VLANs (PVLAN): Use the protect-vlan command to create the protected VLANs that carry normal traffic and are protected by the EAPS ring integrity mechanism. One EAPS domain can be assigned 11 VLANs – control VLAN and 10 protected VLANs. The ring ports of a protected VLAN must be tagged. The protected VLANs will be blocked on the secondary port.

7. Enable or disable EAPS: Before enabling a domain as described in the next step, first use the eaps command to globally enable the EAPS function on the switch. If EAPS has not yet been enabled or has been disabled with the no eaps command, no EAPS domains will work.

8. Enable or disable an EAPS domain: Before an EAPS domain can work, it must be enabled using the enable command. When configuration is completed and the domain is enabled, it will start running on the ring. To stop a domain running on an ring, it can be disabled on any node using the no enable-domain command.

9. Unconfigure an EAPS ring port: Use the no port primary or no port secondary command to unconfigure an EAPS primary or secondary ring port for an EAPS domain.

10. Display EAPS status information: Use the show eaps command to display general EAPS status information or more detailed EAPS status information.

eaps

This command enables EAPS on the switch. Use the **no** form to disable EAPS.

SYNTAX

[**no**] **eaps**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

An EAPS domain containing one Control VLAN and one or more Protected VLANs must be enabled with the enable command, and the EAPS function enabled on the ECN430 with the eaps command before these domains start running on the ring. Once enabled, the master node and transit node state machines will start, and the domain will enter the active state.

EXAMPLE

```
Console(config)#eaps
Console(config)#
```

RELATED COMMANDS

enable (778)

eaps domain

This command creates an EAPS domain and enters EAPS configuration mode for the specified domain. Use the **no** form to delete an EAPS domain.

SYNTAX

[**no**] **eaps domain** *name*

name - Name of a specific EAPS domain. (Range: 1-32 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#eaps domain r&d
Console(config-eaps)#
```

RELATED COMMANDS

show eaps (782)

control-vlan

This command adds a Control VLAN to an EAPS domain. The Control VLAN is used only to send and receive EAPS ring maintenance messages. Use the **no** form to clear the Control VLAN.

SYNTAX

[**no**] **control-vlan** *vlan*-id

vlan-id - VLAN ID (Range: 1-4094, no leading zeroes)

DEFAULT SETTING

None

COMMAND MODE

EAPS Domain Configuration

COMMAND USAGE

- Only one Control VLAN can be configured in an EAPS domain. First create the VLAN to be used as the Control VLAN (vlan, page 805), add the primary and secondary ring ports as tagged members to this VLAN (switchport allowed vlan, page 808), and then use the control-vlan command to add the Control VLAN to the EAPS domain.

- The Control VLAN must not be configured as a Layer 3 interface (with an IP address), a dynamic VLAN (with GVRP enabled), nor as a private VLAN. In addition, only ring ports may be added to the Control VLAN. No other ports can be members of this VLAN. Also, the ring ports of the CVLAN must be tagged. Failure to observe these restrictions can result in a loop in the network.

- Once the domain has been activated with the enable command, the configuration of the Control VLAN cannot be modified. Use the no enable command to stop the EAPS domain before making any configuration changes to this domain.

EXAMPLE

```
Console(config-eaps)#control-vlan 2
Console(config-eaps)#
```

RELATED COMMANDS

protect-vlan (782)

enable

This command enables an EAPS domain. Use the **no** form to disable the EAPS domain.

SYNTAX

[**no**] **enable**

DEFAULT SETTING

Disabled

COMMAND MODE

EAPS Domain Configuration

COMMAND USAGE

An EAPS domain containing one Control VLAN and one or more Protected VLANs must be enabled with the enable command, and the EAPS function enabled on the switch with the eaps command before these domains start running on the ring. Once enabled, the master node and transit node state machines will start, and the domain will enter the active state.

EXAMPLE

```
Console(config-eaps)#enable
Console(config-eaps)#
```

RELATED COMMANDS

eaps (776)

failtime

This command sets the time the master node waits for a health-check packet before declaring a break in the ring.

SYNTAX

failtime *seconds*

seconds - The interval at which the master node sends health-check packets. (Range: 3-9 seconds)

DEFAULT SETTING
3 seconds

COMMAND MODE
EAPS Domain Configuration

COMMAND USAGE
- The fail time should be set on the master node. Once set, the master node sends the newly configured fail time to all transit nodes, forcing each node to update its fail timer. On transit nodes, the default value for the fail time can be used until receiving a control message with the configured fail time.

  The transit nodes check for a health-check packet at the interval specified by the fail time, and report a link down event to the master node if a health-check packet is not received during this interval.

  If the master node receives a link-down event message from a transit node, or does not receive the health-check frame before the fail timer expires, the master node moves from the normal state to the "ring-fault" state and unblocks its secondary port. The master node also flushes its bridging table and sends a control frame to all other nodes, instructing them to also flush their bridging tables. Immediately after flushing its bridge table, each node starts learning the new topology.

  This ring polling mechanism provides a backup in the event that the link-down alert frame should get lost for some unforeseen reason.

- The failover time should always be set to a value greater than the interval specified by the hellotime command.

EXAMPLE
```
Console(config-eaps)#failtime 9
Console(config-eaps)#
```

RELATED COMMANDS
hellotime (779)

hellotime
This command sets the interval at which the master node sends health-check packets on the domain ring.

SYNTAX
hellotime *seconds*

seconds - The interval at which the master node sends health-check packets. (Range: 1-3 seconds)

DEFAULT SETTING
1 second

COMMAND MODE
EAPS Domain Configuration

COMMAND USAGE
The hello time should be set on the master node. Once set, the master node will send a health-check packet at the interval specified by this timer to all transit nodes. The transit nodes check for a health-check packet at the interval specified by the failtime command. Therefore, the hello time should always be set to a value less than the failover time.

EXAMPLE

```
Console(config-eaps)#hellotime 2
Console(config-eaps)#
```

RELATED COMMANDS
failtime (778)

mode
This command configures the switch as a master node or transit node on the ring.

SYNTAX
mode {**master** | **transit**}

master - Configures the switch as the master node of the EAPS domain. This node actively monitors ring integrity and sends health check and state change messages to transit nodes. Only one master node can be set for a domain.

transit - Configures the switch as a transit node in the EAPS domain. Transit nodes receive master control messages, detect ring topology changes, and send status messages to the master node.

DEFAULT SETTING
None

COMMAND MODE
EAPS Domain Configuration

COMMAND USAGE
- The master node is the control node of the EAPS domain.
- The transit node will receive control messages from the master node to synchronize the hello and fail timers. All other configuration parameters for a transit node should be configured to be the same as that of the EAPS domain's master node.

EXAMPLE

```
Console(config-eaps)#mode master
Console(config-eaps)#
```

RELATED COMMANDS
port (781)

port

This command sets the port type attached to the ring as primary or secondary. Each node must connect to the ring through two ports as part of the protection switching scheme – one port as the primary port and another as the secondary port. Use the no form to remove a primary or secondary port from the ring.

SYNTAX

port {**primary** | **secondary**} *port-number*

no port {**primary** | **secondary**}

primary - This port is open on the Protected VLAN and is used for passing both control messages and data traffic. The master node sends control messages from this port.

secondary - This port is blocked on the Protected VLAN and is used only to receive control messages on the master node.

port-number - Range: 1-28/52

DEFAULT SETTING
None

COMMAND MODE
EAPS Domain Configuration

COMMAND USAGE
- If the ring is complete, the master node prevents a loop by logically blocking all data traffic in the transmit and receive directions on its secondary port. If the master node subsequently detects a break in the ring, it unblocks its secondary port and allows data traffic to be transmitted and received through it.
- The primary port and secondary port must be removed from an EAPS domain with the **no port** command, before specifying a new primary or secondary port.

EXAMPLE

```
Console(config-eaps)#port primary 24
Console(config-eaps)#port secondary 25
Console(config-eaps)#
```

protect-vlan

This command adds a Protected VLAN to an EAPS domain. Protected VLANs are used to send and receive data traffic on the EAPS ring. Use the **no** form to clear the Protected VLANs.

SYNTAX

[**no**] **protect-vlan** *vlan*-id

vlan-id - VLAN ID (Range: 1-4094, no leading zeroes)

DEFAULT SETTING

None

COMMAND MODE

EAPS Domain Configuration

COMMAND USAGE

- Up to 10 Protected VLANs can be configured in an EAPS domain. First create the VLANs to be used as Protected VLANs (vlan, page 805), add the primary and secondary ring ports as tagged members to this VLAN (switchport allowed vlan, page 808), and then use the **protect-vlan** command to add the Protected VLAN to the EAPS domain.
- Once the domain has been activated with the enable command, the configuration of the Protected VLAN cannot be modified. Use the no enable command to stop the EAPS domain before making any configuration changes to this domain.

EXAMPLE

```
Console(config-eaps)#protect-vlan 246
Console(config-eaps)#protect-vlan 247
Console(config-eaps)#protect-vlan 248
Console(config-eaps)#
```

RELATED COMMANDS

control-vlan (777)

show eaps

This command displays status information for configured EAPS domains.

SYNTAX

show eaps [*domain-name*]

domain-name - Name of a specific EAPS domain. (Range: 1-32 characters)

COMMAND MODE

Privileged Exec

COMMAND USAGE

- Enter the **show eaps** command without any argument to display a summary of status information for all configured EAPS domains.
- Enter the **show eaps** command followed by a domain name to display detailed status information for the specified domain.

EXAMPLE

This example displays a summary of all the EAPS domains configured on the switch.

```
Console#show eaps
EAPS Status            : Enabled
Number of EAPS Domains : 1

Domain       State         Mode Enabled Pri Port Sec Port Ctrl VLAN VLAN count
------------ ------------- ---- ------- -------- -------- --------- ----------
r&d          Init          M       Y    Eth 1/24 Eth 1/25         2          3

Console#
```

Table 107: **show eaps** - summary display description

Field	Description
EAPS Status	Shows whether EAPS is enabled on the switch.
Number of EAPS Domains	Shows the number of EAPS domains configured on the switch.
Domain	Displays the name of each domain followed by a brief list of status information
State	Shows the following EAPS states: *Master Node* Idle – The EAPS domain has been enabled, but the configuration is not complete. Init – The EAPS domain has started but has not yet determined the status of the ring. Complete – The ring is in the COMPLETE state for this EAPS domain. Failed – There is a break in the ring for this EAPS domain. *Transit Node* Idle – The EAPS domain has been enabled, but the configuration is not complete. Link-Up – The EAPS domain is running, and both of its ports are up and in the FORWARDING state. Link-Down – This EAPS domain is running, but one or both of its ports are down. Preforwarding – This EAPS domain is running, and both of its ports are up, but the new link port is in a temporary BLOCKED state.
Mode	Shows if the switch is a master or transit node.
Enabled	Shows if the specified domain is enabled.
Pri Port	Shows the primary port.
Sec Port	Shows the secondary port.
Ctrl VLAN	Shows the Control VLAN ID.
VLAN count	Shows the number of Protected VLANs in this domain.

This example displays detailed information for the specified EAPS domain.

```
Console#show eaps r&d
Name                          : r&d
Admin Status                  : Enabled
State                         : Init
Mode                          : Master
Primary Port                  : Eth 1/24      Port Status : Down
Secondary Port                : Eth 1/25      Port Status : Down
Hello Timer Interval          : 2 seconds
Fail Timer Interval           : 3 seconds
Control VLAN                  : 2
Protected VLAN(s)             : 246, 247, 248

Console#
```

Table 108: **show eaps** - detailed display description

Field	Description
Name	The EAPS domain name.
Admin Status	Shows if the specified domain is enabled.
State	See Table 107.
Mode	Shows if the switch is a master or transit node.
Primary Port	Shows the primary port and its operational status, where potential port states include Init, Complete, Failed or Down.
Secondary Port	Shows the secondary port and its operational status.
Hello Timer Interval	The interval at which the master node sends health-check packets on the domain ring.
Fail Timer Interval	The time the master node waits for a health-check packet before declaring a break in the ring.
Control VLAN	Shows the VLAN ID of the Control VLAN.
Protected VLAN(s)	Shows the VLAN IDs of the Protected VLANs.

36 ERPS COMMANDS

NOTE: Information in this section is based on ITU-T G.8032/Y.1344.

The ITU G.8032 recommendation specifies a protection switching mechanism and protocol for Ethernet layer network rings. Ethernet rings can provide wide-area multipoint connectivity more economically due to their reduced number of links. The mechanisms and protocol defined in G.8032 achieve highly reliable and stable protection; and never form loops, which would fatally affect network operation and service availability.

The G.8032 recommendation, also referred to as Ethernet Ring Protection Switching (ERPS), can be used to increase the availability and robustness of Ethernet rings. An Ethernet ring built using ERPS can provide resilience at a lower cost and than that provided by SONET or EAPS rings.

ERPS is more economical than EAPS in that only one physical link is required between each node in the ring. However, since it can tolerate only one break in the ring, it is not as robust as EAPS. ERPS supports up to 255 nodes in the ring structure. ERPS requires a higher convergence time when more that 16 nodes are used, but should always run under than 500 ms.

Operational Concept

Loop avoidance in the ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links. This particular link is called the ring protection link (RPL), and under normal conditions this link is blocked to traffic. One designated node, the RPL owner, is responsible for blocking traffic over the RPL. When a ring failure occurs, the RPL owner is responsible for unblocking the RPL, allowing this link to be used for traffic.

Ring nodes may be in one of two states:

Idle – normal operation, no link/node faults detected in ring
Protection – Protection switching in effect after identifying a signal fault

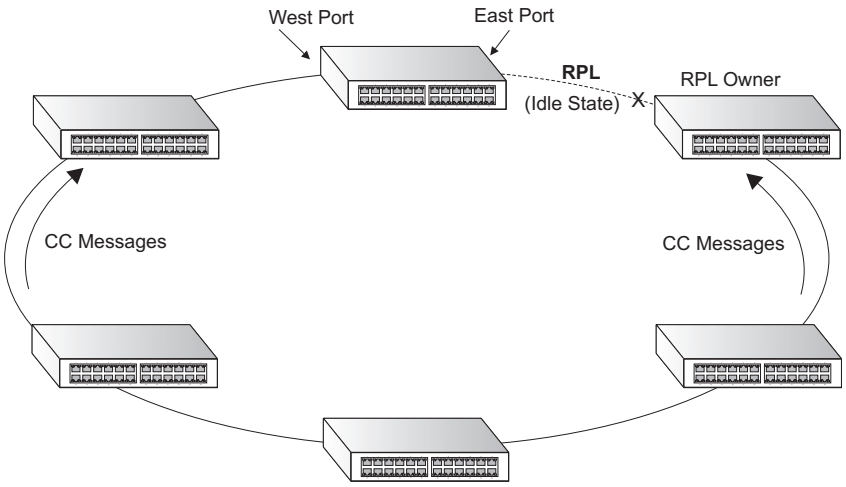
In Idle state, the physical topology has all nodes connected in a ring. The logical topology guarantees that all nodes are connected without a loop by blocking the RPL. Each link is monitored by its two adjacent nodes using Connectivity Fault Management (CFM) protocol messages.

Protection switching (opening the RPL to traffic) occurs when a signal failure message generated by the Connectivity Fault Management (CFM) protocol is declared on one of the ring links, and the detected failure has a higher priority than any other request; or a Ring – Automatic Protection

Switching protocol request (R-APS, as defined in Y.1731) is received which has a higher priority than any other local request.

A link/node failure is detected by the nodes adjacent to the failure. These nodes block the failed link and report the failure to the ring using R-APS (SF) messages. This message triggers the RPL owner to unblock the RPL, and all nodes to flush their forwarding database. The ring is now in protection state, but it remains connected in a logical topology.

When the failed link recovers, the traffic is kept blocked on the nodes adjacent to the recovered link. The nodes adjacent to the recovered link transmit R-APS(NR - no request) message indicating they have no local request. When the RPL owner receives an R-APS(NR) message it starts the Wait-To-Recover (WTR) timer. Once WTR timer expires, the RPL owner blocks the RPL and transmits an R-APS (NR, RB - ring blocked) message. Nodes receiving this message flush the forwarding database and unblock their previously blocked ports. The ring is now returned to Idle state.



Configuration Limitations for ERPS

The following configuration limitations apply to ERPS:

- One switch only supports two ERPS rings – each ring must have one Control VLAN, and at most 255 Data VLANs.
- Ring ports can not be a member of a dynamic trunk.
- Dynamic VLANs are not supported as protected data ports.
- Exclusive use of STP, EAPS or ERPS on any port.
- The switch takes about 350 ms to detect link-up on 1000Base-T copper ports, so the convergence time on this port type is more than 50 ms.

- One VLAN must be added to an EAPS domain as the CVLAN. This can be designated as any VLAN, other than the management VLAN. The CVLAN should only contain ring ports, and must not be configured with an IP address.

This section describes commands used to configure ERPS.

Table 109: ERPS Commands

Command	Function	Mode
erps	Enables ERPS globally on the switch	GC
erps domain	Creates an ERPS ring and enters ERPS configuration mode	GC
control-vlan	Adds a Control VLAN to an ERPS ring	ERPS
enable	Activates the current ERPS ring	ERPS
guard-timer	Sets the timer to prevent ring nodes from receiving outdated R-APS messages	ERPS
holdoff-timer	Sets the timer to filter out intermittent link faults	ERPS
meg-level	Sets the Maintenance Entity Group level for a ring	ERPS
node-id	Sets the MAC address for a ring node	ERPS
ring-port	Configures a node's connection to the ring through the east or west interface	ERPS
rpl owner	Configures a ring node to be the RPL owner or a non-owner	ERPS
wtr-timer	Sets timer to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure	ERPS
show erps	Displays status information for all configured rings, or for a specified ring	PE

Configuration Guidelines for ERPS

1. Create an ERPS ring: Create a ring using the erps domain command. The ring name is used as an index in the G.8032 database.

2. Configure the east and west interfaces: Each node on the ring connects to it through two ring ports. Use the ring-port command to configure one port connected to the next node in the ring to the east (or clockwise direction); and then use the ring-port command again to configure another port facing west in the ring.

3. Configure the RPL owner: Configure one node in the ring as the Ring Protection Link (RPL) owner using the rpl owner command. When this switch is configured as the RPL owner, the west ring port is set as being connected to the RPL. Under normal operations (Idle state), the RPL is blocked to ensure that a loop cannot form in the ring. If a signal failure brings down any other link in the ring, the RPL will be unblocked (Protection state) to ensure proper connectivity among all ring nodes until the failure is recovered.

4. Configure ERPS timers: Use the guard-timer command to set the timer is used to prevent ring nodes from receiving outdated R-APS messages, the holdoff-timer command to filter out intermittent link faults, and the

wtr-timer command to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure.

5. Configure the ERPS Control VLAN (CVLAN): Use the control-vlan command to create the VLAN used to pass R-APS ring maintenance commands. The CVLAN must NOT be configured with an IP address. In addition, only ring ports may be added to the CVLAN (prior to configuring the VLAN as a CVLAN). No other ports can be members of this VLAN (once set as a CVLAN). Also, the ring ports of the CVLAN must be tagged. Failure to observe these restrictions can result in a loop in the network.

6. Enable ERPS: Before enabling a ring as described in the next step, first use the erps command to globally enable ERPS on the switch. If ERPS has not yet been enabled or has been disabled with the no erps command, no ERPS rings will work.

7. Enable an ERPS ring: Before an EAPS ring can work, it must be enabled using the enable command. When configuration is completed and the ring enabled, R-APS messages will start flowing in the control VLAN, and normal traffic will begin to flow in the data VLANs. To stop a ring, it can be disabled on any node using the no enable command.

8. Display ERPS status information: Use the show erps command to display general ERPS status information or detailed ERPS status information for a specific ring.

erps

This command enables ERPS on the switch. Use the **no** form to disable this feature.

SYNTAX

[**no**] **erps**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

ERPS must be enabled globally on the switch before it can enabled on an ERPS ring using the enable command.

EXAMPLE

```
Console(config)#erps
Console(config)#
```

RELATED COMMANDS

enable (790)

erps domain

This command creates an ERPS ring and enters ERPS configuration mode for the specified domain. Use the **no** form to delete a ring.

SYNTAX

[**no**] **eaps domain** *name*

name - Name of a specific ERPS ring. (Range: 1-32 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#erps domain r&d
Console(config-eaps)#
```

control-vlan

This command specifies a dedicated VLAN used for sending and receiving E-APS protocol messages. Use the **no** form to remove the Control VLAN.

SYNTAX

[**no**] **control-vlan** *vlan*-id

vlan-id - VLAN ID (Range: 1-4094, no leading zeroes)

DEFAULT SETTING

None

COMMAND MODE

ERPS Configuration

COMMAND USAGE

- Configure one control VLAN for each ERPS ring. First create the VLAN to be used as the control VLAN (vlan, page 805), add the ring ports for the east and west interface as tagged members to this VLAN (switchport allowed vlan, page 808), and then use the control-vlan command to add it to the ring.
- The Control VLAN must not be configured as a Layer 3 interface (with an IP address), a dynamic VLAN (with GVRP enabled), nor as a private VLAN. In addition, only ring ports may be added to the Control VLAN. No other ports can be members of this VLAN. Also, the ring ports of the Control VLAN must be tagged. Failure to observe these restrictions can result in a loop in the network.
- Once the ring has been activated with the enable command, the configuration of the control VLAN cannot be modified. Use the no enable command to stop the ERPS ring before making any configuration changes to the control VLAN.

EXAMPLE

```
Console(config)#vlan database
Console(config-vlan)#vlan 2 name rdc media ethernet state active
Console(config-vlan)#exit
Console(config)#interface ethernet 1/21
Console(config-if)#switchport allowed vlan add 2 tagged
Console(config-if)#interface ethernet 1/22
Console(config-if)#switchport allowed vlan add 2 tagged
Console(config-if)#exit
Console(config)#erps domain rd1
Console(config-erps)#control-vlan 2
Console(config-erps)#
```

enable

This command activates the current ERPS ring. Use the **no** form to disable the current ring.

SYNTAX

[**no**] **enable**

DEFAULT SETTING

Disabled

COMMAND MODE

ERPS Configuration

COMMAND USAGE

- Before enabling a ring, the global ERPS function should be enabled with the erps command, the east and west ring ports configured on each node with the ring-port command, the RPL owner specified with the rpl owner command, and the control VLAN configured with the control-vlan command.
- Once enabled, the RPL owner node and non-owner node state machines will start, and the ring will enter idle state if no signal failures are detected.

EXAMPLE

```
Console(config-erps)#enable
Console(config-erps)#
```

RELATED COMMANDS

erps (788)

guard-timer

This command sets the guard timer to prevent ring nodes from receiving outdated R-APS messages. Use the **no** form to restore the default setting.

SYNTAX

guard-timer *milliseconds*

milliseconds - The guard timer is used to prevent ring nodes from receiving outdated R-APS messages. During the duration of the guard timer, all received R-APS messages are ignored by the ring protection control process, giving time for old messages still circulating on the ring to expire. (Range: 10-2000 milliseconds, in steps of 10 milliseconds)

DEFAULT SETTING

500 milliseconds

COMMAND MODE

ERPS Configuration

COMMAND USAGE

The guard timer duration should be greater than the maximum expected forwarding delay for an R-APS message to pass around the ring. A side-effect of the guard timer is that during its duration, a node will be unaware of new or existing ring requests transmitted from other nodes.

EXAMPLE

```
Console(config-erps)#guard-timer 300
Console(config-erps)#
```

holdoff-timer

This command sets the timer to filter out intermittent link faults. Use the **no** form to restore the default setting.

SYNTAX

holdoff-timer *milliseconds*

milliseconds - The hold-off timer is used to filter out intermittent link faults. Faults will only be reported to the ring protection mechanism if this timer expires. (Range: 0-10000 milliseconds, in steps of 100 milliseconds)

DEFAULT SETTING

0 milliseconds

COMMAND MODE

ERPS Configuration

COMMAND USAGE

In order to coordinate timing of protection switches at multiple layers, a hold-off timer may be required. Its purpose is to allow, for example, a

server layer protection switch to have a chance to fix the problem before switching at a client layer.

When a new defect or more severe defect occurs (new Signal Failure), this event will not be reported immediately to the protection switching mechanism if the provisioned hold-off timer value is non-zero. Instead, the hold-off timer will be started. When the timer expires, whether a defect still exists or not, the timer will be checked. If one does exist, that defect will be reported to the protection switching mechanism. The reported defect need not be the same one that started the timer.

EXAMPLE

```
Console(config-erps)#holdoff-timer 300
Console(config-erps)#
```

meg-level

This command sets the Maintenance Entity Group level for a ring. Use the **no** form to restore the default setting.

SYNTAX

meg-level *level*

level - The maintenance entity group (MEG) level which provides a communication channel for ring automatic protection switching (R-APS) information. (Range: 0-7)

DEFAULT SETTING

1

COMMAND MODE

ERPS Configuration

COMMAND USAGE

This parameter is used to ensure that received R-APS PDUs are directed for this ring. A unique level should be configured for each local ring if there are many R-APS PDUs passing through this switch.

EXAMPLE

```
Console(config-erps)#meg-level 00-12-CF-61-24-2D
Console(config-erps)#
```

node-id

This command sets the MAC address for a ring node. Use the **no** form to restore the default setting.

SYNTAX

node-id *mac-address*

mac-address – A MAC address unique to the ring node. The MAC address must be specified in the format xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.

DEFAULT SETTING

CPU MAC address

COMMAND MODE

ERPS Configuration

COMMAND USAGE

The ring node identifier is informational, and does not affect ring protection switching operations. It may be used for debugging, such as to distinguish messages when a node is connected to more than one ring.

EXAMPLE

```
Console(config-erps)#node-id 00-12-CF-61-24-2D
Console(config-erps)#
```

ring-port

This command configures a node's connection to the ring through the east or west interface. Use the **no** form to disassociate a node from the ring.

SYNTAX

ring-port {**east** | **west**} *interface*

east - Connects to next ring node to the east.

west - Connects to next ring node to the west.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* - The assigned number of a static aggregated link. (Range: 1-8)

DEFAULT SETTING

Not associated

COMMAND MODE

ERPS Configuration

COMMAND USAGE

Each node must be connected to two neighbors on the ring. For convenience, the ports connected are referred to as east and west ports. Alternatively, the closest neighbor to the east should be the next node in the ring in a clockwise direction, and the closest neighbor to the west should be the next node in the ring in a counter-clockwise direction.

EXAMPLE

```
Console(config-erps)#ring-port east interface ethernet 1/21
Console(config-erps)#
```

rpl owner

This command configures a ring node to be the Ring Protection Link (RPL) owner or a non-owner.

SYNTAX

[**no**] **rpl owner**

DEFAULT SETTING

non-owner

COMMAND MODE

ERPS Configuration

COMMAND USAGE

- Only one RPL owner can be configured on a ring. The owner blocks traffic on the RPL during Idle state, and unblocks it during Protection state (that is, when a signal fault is detected on the ring).
- The east and west connections to the ring must be specified for all ring nodes using the ring-port command. When this switch is configured as the RPL owner, the west ring port is set as being connected to the RPL.

EXAMPLE

```
Console(config-erps)#rpl owner
Console(config-erps)#
```

wtr-timer

This command sets the wait-to-restore timer which is used to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure. Use the **no** form to restore the default setting.

SYNTAX

wtr-timer *minutes*

minutes - The wait-to-restore timer is used to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure. (Range: 5-12 minutes)

DEFAULT SETTING
5 minutes

COMMAND MODE
ERPS Configuration

COMMAND USAGE
If the switch goes into ring protection state due to a signal failure, after the failure condition is cleared, the RPL owner will start the wait-to-restore timer and wait until it expires to verify that the ring has stabilized before blocking the RPL and returning to the Idle (normal operating) state.

EXAMPLE

```
Console(config-erps)#wtr-timer 10
Console(config-erps)#
```

show erps

This command displays status information for all configured rings, or for a specified ring

SYNTAX

show erps [**domain** *ring-name*]

ring-name - Name of a specific ERPS ring. (Range: 1-32 characters)

COMMAND MODE
Privileged Exec

EXAMPLE
This example displays a summary of all the ERPS rings configured on the switch.

```
Console#show erps
ERPS Status             : Enabled
Number of ERPS Domains  : 1

Domain       State      MEL Enabled West     East     RPL Owner Ctrl VLAN
------------ ---------- --- ------- -------- -------- --------- ---------
rd1          Idle         0 Yes     Eth 1/20 Eth 1/10 Yes             100
rd2          Protection   0 Yes     Eth 1/3  Eth 1/4  No               200
Console#
```

Table 110: **show erps** - summary display description

Field	Description
ERPS Status	Shows whether ERPS is enabled on the switch.
Number of ERPS Domains	Shows the number of ERPS rings configured on the switch.
Domain	Displays the name of each ring followed by a brief list of status information

Table 110: **show erps** - summary display description (Continued)

Field	Description
State	Shows the following ERPS states: Init – The ERPS ring has started but has not yet determined the status of the ring. Idle – If all nodes in a ring are in this state, it means that all the links in the ring are up. This state will switch to protection state if a link failure occurs. Protection – If a node in this state, it means that a link failure has occurred. This state will switch to idle state if all the failed links recover.
MEL	The maintenance entity group (MEG) level providing a communication channel for ring automatic protection switching (R-APS) information.
Enabled	Shows if the ring is enabled.
West	Shows the west ring port for this node.
East	Shows the east ring port for this node.
RPL Owner	Shows if this node is the RPL owner.
Ctrl VLAN	Shows the Control VLAN ID.

This example displays detailed information for the specified ERPS ring.

```
Console#show erps domain rd1
Domain Name    : rd1
Admin Status   : Enabled
MEG Level      : 1
Node ID        : 00-12-CF-61-24-2F
Node State     : Idle
West Port      : Eth 1/ 1 (Blocking)
East Port      : Eth 1/ 2 (Forwarding)
RPL Port       : West
RPL Owner      : Enabled
Holdoff Timer  : 300 ms
Guard Timer    : 300 ms
WTR Timer      : 5 minutes
Control VLAN   : 2

Console#
```

Table 111: **show erps domain** - detailed display description

Field	Description
Domain Name	The ERPS ring name.
Admin Status	Shows if the specified ring is enabled.
MEG Level	The maintenance entity group (MEG) level providing a communication channel for ring automatic protection switching (R-APS) information.
Node ID	A MAC address unique to this ring node.
Node State	See Table 110.

Table 111: **show erps domain** - detailed display description (Continued)

Field	Description
West Port	Shows the west ring port for this node, and the interface state: Blocking – The transmission and reception of traffic is blocked and the forwarding of R-APS messages is blocked, but the transmission of locally generated R-APS messages is allowed and the reception of all R-APS messages is allowed. Forwarding – The transmission and reception of traffic is allowed; transmission, reception and forwarding of R-APS messages is allowed. Down – The interface is not linked up.
East Port	Shows the west ring port for this node, and the interface state as described in the preceding item.
RPL Port	If node is connected to the RPL, this shows by which interface.
RPL Owner	Shows if this node is the RPL owner.
Holdoff Timer	The hold-off timer interval used to filter out intermittent link faults.
Guard Timer	The guard timer interval used to prevent ring nodes from receiving outdated R-APS messages.
WTR Timer	The wait-to-restore timer interval used to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure.
Control VLAN	Shows the ID of the Control VLAN.

37 VLAN COMMANDS

A VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. This section describes commands used to create VLAN groups, add port members, specify how VLAN tagging is used, and enable automatic VLAN registration for the selected interface.

Table 112: VLAN Commands

Command Group	Function
GVRP and Bridge Extension Commands	Configures GVRP settings that permit automatic VLAN learning; shows the configuration for bridge extension MIB
Editing VLAN Groups	Sets up VLAN groups, including name, VID and state
Configuring VLAN Interfaces	Configures VLAN interface parameters, including ingress and egress tagging mode, ingress filtering, PVID, and GVRP
Displaying VLAN Information	Displays VLAN groups, status, port members, and MAC addresses
Configuring IEEE 802.1Q Tunneling	Configures 802.1Q Tunneling (QinQ Tunneling)
Configuring Port-based Traffic Segmentation	Configures traffic segmentation for different client sessions based on specified downlink and uplink ports
Configuring Private VLANs	Configures private VLANs, including uplink and downlink ports
Configuring Protocol-based VLANs	Configures protocol-based VLANs based on frame type and protocol
Configuring IP Subnet VLANs	Configures IP Subnet-based VLANs
Configuring MAC Based VLANs	Configures MAC-based VLANs
Configuring Voice VLANs	Configures VoIP traffic detection and enables a Voice VLAN

GVRP AND BRIDGE EXTENSION COMMANDS

GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network. This section describes how to enable GVRP for individual interfaces and globally for the switch, as well as how to display default configuration settings for the Bridge Extension MIB.

Table 113: GVRP and Bridge Extension Commands

Command	Function	Mode
bridge-ext gvrp	Enables GVRP globally for the switch	GC
garp timer	Sets the GARP timer for the selected function	IC
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC
switchport gvrp	Enables GVRP for an interface	IC
show bridge-ext	Shows the global bridge extension configuration	PE
show garp timer	Shows the GARP timer for the selected function	NE, PE
show gvrp configuration	Displays GVRP configuration for the selected interface	NE, PE

bridge-ext gvrp

This command enables GVRP globally for the switch. Use the **no** form to disable it.

SYNTAX

[**no**] **bridge-ext gvrp**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

GVRP defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. This function should be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

EXAMPLE

```
Console(config)#bridge-ext gvrp
Console(config)#
```

garp timer

This command sets the values for the join, leave and leaveall timers. Use the **no** form to restore the timers' default values.

SYNTAX

garp timer {**join** | **leave** | **leaveall**} *timer-value*

no garp timer {**join** | **leave** | **leaveall**}

{**join** | **leave** | **leaveall**} - Timer to set.

timer-value - Value of timer.
Ranges:
join: 20-1000 centiseconds
leave: 60-3000 centiseconds
leaveall: 500-18000 centiseconds

DEFAULT SETTING

join: 20 centiseconds
leave: 60 centiseconds
leaveall: 1000 centiseconds

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- Group Address Registration Protocol is used by GVRP and GMRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GMRP or GVRP registration/deregistration.
- Timer values are applied to GVRP for all the ports on all VLANs.
- Timer values must meet the following restrictions:
  - leave >= (2 x join)
  - leaveall > leave

NOTE: Set GVRP timers on all Layer 2 devices connected in the same network to the same values. Otherwise, GVRP may not operate successfully.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#garp timer join 100
Console(config-if)#
```

RELATED COMMANDS

show garp timer (803)

switchport forbidden vlan

This command configures forbidden VLANs. Use the **no** form to remove the list of forbidden VLANs.

SYNTAX

switchport forbidden vlan {**add** *vlan-list* | **remove** *vlan-list*}

no switchport forbidden vlan

add *vlan-list* - List of VLAN identifiers to add.

remove *vlan-list* - List of VLAN identifiers to remove.

vlan-list - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4094).

DEFAULT SETTING

No VLANs are included in the forbidden list.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- This command prevents a VLAN from being automatically added to the specified interface via GVRP.
- If a VLAN has been added to the set of allowed VLANs for an interface, then you cannot add it to the set of forbidden VLANs for that same interface.

EXAMPLE

The following example shows how to prevent port 1 from being added to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```

switchport gvrp

This command enables GVRP for a port. Use the **no** form to disable it.

SYNTAX

[**no**] **switchport gvrp**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport gvrp
Console(config-if)#
```

show bridge-ext

This command shows the configuration for bridge extension commands.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

See "Displaying Bridge Extension Capabilities" for a description of the displayed items.

EXAMPLE

```
Console#show bridge-ext
 Maximum Supported VLAN Numbers        : 4092
 Maximum Supported VLAN ID             : 4094
 Extended Multicast Filtering Services : No
 Static Entry Individual Port          : Yes
 VLAN Learning                         : IVL
 Configurable PVID Tagging             : Yes
 Local VLAN Capable                    : No
 Traffic Classes                       : Enabled
 Global GVRP Status                    : Disabled
 GMRP                                  : Disabled
Console#
```

show garp timer

This command shows the GARP timers for the selected interface.

SYNTAX

show garp timer [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

Shows all GARP timers.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
Console#show garp timer ethernet 1/1
Eth 1/ 1 GARP Timer Status:
 Join Timer:     20 centiseconds
 Leave Timer:    60 centiseconds
 Leaveall Timer: 1000 centiseconds
Console#
```

RELATED COMMANDS

garp timer (801)

show gvrp configuration

This command shows if GVRP is enabled.

SYNTAX

show gvrp configuration [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

Shows both global and interface-specific configuration.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
Console#show gvrp configuration ethernet 1/7
Eth 1/ 7:
 GVRP Configuration : Disabled
Console#
```

EDITING VLAN GROUPS

Table 114: Commands for Editing VLAN Groups

Command	Function	Mode
vlan database	Enters VLAN database mode to add, change, and delete VLANs	GC
vlan	Configures a VLAN, including VID, name and state	VC

vlan database

This command enters VLAN database mode. All commands in this mode will take effect immediately.

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- Use the VLAN database command mode to add, change, and delete VLANs. After finishing configuration changes, you can display the VLAN settings by entering the show vlan command.
- Use the interface vlan command mode to define the port membership mode and add or remove ports from a VLAN. The results of these commands are written to the running-configuration file, and you can display this file by entering the show running-config command.

EXAMPLE

```
Console(config)#vlan database
Console(config-vlan)#
```

RELATED COMMANDS

show vlan (813)

vlan

This command configures a VLAN. Use the **no** form to restore the default settings or delete a VLAN.

SYNTAX

vlan *vlan-id* [**name** *vlan-name*] **media ethernet** [**state** {**active** | **suspend**}]

no vlan *vlan-id* [**name** | **state**]

vlan-id - VLAN ID, specified as a single number, a range of consecutive numbers separated by a hyphen, or multiple numbers separated by commas. (Range: 1-4094, no leading zeroes)

name - Keyword to be followed by the VLAN name.

vlan-name - ASCII string from 1 to 128 characters.

media ethernet - Ethernet media type.

state - Keyword to be followed by the VLAN state.

active - VLAN is operational.

suspend - VLAN is suspended. Suspended VLANs do not pass packets.

DEFAULT SETTING
By default only VLAN 1 exists and is active.

COMMAND MODE
VLAN Database Configuration

COMMAND USAGE
- **no vlan** *vlan-id* deletes the VLAN.
- **no vlan** *vlan-id* **name** removes the VLAN name.
- **no vlan** *vlan-id* **state** returns the VLAN to the default state (i.e., active).
- You can configure up to 255 VLANs on the switch.

NOTE: The switch allows 255 user-manageable VLANs. One extra, unmanageable VLAN (VLAN ID 4093) is maintained for switch clustering.

EXAMPLE
The following example adds a VLAN, using VLAN ID 105 and name RD5. The VLAN is activated by default.

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

RELATED COMMANDS
show vlan (813)

CONFIGURING VLAN INTERFACES

Table 115: Commands for Configuring VLAN Interfaces

Command	Function	Mode
interface vlan	Enters interface configuration mode for a specified VLAN	IC
switchport acceptable-frame-types	Configures frame types to be accepted by an interface	IC
switchport allowed vlan	Configures the VLANs associated with an interface	IC
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC
switchport gvrp	Enables GVRP for an interface	IC
switchport ingress-filtering	Enables ingress filtering on an interface	IC
switchport mode	Configures VLAN membership mode for an interface	IC
switchport native vlan	Configures the PVID (native VLAN) of an interface	IC

Table 115: Commands for Configuring VLAN Interfaces (Continued)

Command	Function	Mode
switchport priority default	Sets a port priority for incoming untagged frames	IC
vlan-trunking	Allows unknown VLANs to cross the switch	IC

interface vlan

This command enters interface configuration mode for VLANs, which is used to configure VLAN parameters for a physical interface.

SYNTAX

[**no**] **interface vlan** *vlan-id*

vlan-id - ID of the configured VLAN. (Range: 1-4094, no leading zeroes)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

EXAMPLE

The following example shows how to set the interface configuration mode to VLAN 1, and then assign an IP address to the VLAN:

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

RELATED COMMANDS

shutdown (688)
interface (682)
vlan (805)

switchport acceptable-frame-types

This command configures the acceptable frame types for a port. Use the **no** form to restore the default.

SYNTAX

switchport acceptable-frame-types {**all** | **tagged**}

no switchport acceptable-frame-types

all - The port accepts all frames, tagged or untagged.

tagged - The port only receives tagged frames.

DEFAULT SETTING

All frame types

COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE
When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN.

EXAMPLE
The following example shows how to restrict the traffic received on port 1 to tagged frames:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

RELATED COMMANDS
switchport mode (810)

switchport allowed vlan

This command configures VLAN groups on the selected interface. Use the **no** form to restore the default.

SYNTAX

switchport allowed vlan {**add** *vlan-list* [**tagged** | **untagged**] | **remove** *vlan-list*}

no switchport allowed vlan

add *vlan-list* - List of VLAN identifiers to add.

remove *vlan-list* - List of VLAN identifiers to remove.

vlan-list - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4094).

DEFAULT SETTING
All ports are assigned to VLAN 1 by default.
The default frame type is untagged.

COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE
- A port, or a trunk with switchport mode set to **hybrid**, must be assigned to at least one VLAN as untagged.
- If a trunk has switchport mode set to **trunk** (i.e., 1Q Trunk), then you can only assign an interface to VLAN groups as a tagged member.

- Frames are always tagged within the switch. The tagged/untagged parameter used when adding a VLAN to an interface tells the switch whether to keep or remove the tag from a frame on egress.
- If none of the intermediate network devices nor the host at the other end of the connection supports VLANs, the interface should be added to these VLANs as an untagged member. Otherwise, it is only necessary to add at most one VLAN as untagged, and this should correspond to the native VLAN for the interface.
- If a VLAN on the forbidden list for an interface is manually added to that interface, the VLAN is automatically removed from the forbidden list for that interface.

EXAMPLE

The following example shows how to add VLANs 1, 2, 5 and 6 to the allowed list as tagged VLANs for port 1:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 1,2,5,6 tagged
Console(config-if)#
```

switchport ingress-filtering

This command enables ingress filtering for an interface. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **switchport ingress-filtering**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- Ingress filtering only affects tagged frames.
- If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).
- If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
- Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STA. However, they do affect VLAN dependent BPDU frames, such as GMRP.

EXAMPLE

The following example shows how to set the interface to port 1 and then enable ingress filtering:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

switchport mode

This command configures the VLAN membership mode for a port. Use the **no** form to restore the default.

SYNTAX

switchport mode {**access** | **hybrid** | **trunk** | **private-vlan**}

no switchport mode

access - Specifies an access VLAN interface. The port transmits and receives untagged frames on a single VLAN only.

hybrid - Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.

trunk - Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. Note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are also transmitted as tagged frames.

private-vlan - For an explanation of this command see the switchport mode private-vlan command.

DEFAULT SETTING

All ports are in access mode with the PVID set to VLAN 1.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

Access mode is mutually exclusive with VLAN trunking (see the vlan-trunking command). If VLAN trunking is enabled on an interface, then that interface cannot be set to access mode, and vice versa.

EXAMPLE

The following shows how to set the configuration mode to port 1, and then set the switchport mode to hybrid:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

RELATED COMMANDS

switchport acceptable-frame-types (807)

switchport native vlan

This command configures the PVID (i.e., default VLAN ID) for a port. Use the **no** form to restore the default.

SYNTAX

switchport native vlan *vlan-id*

no switchport native vlan

vlan-id - Default VLAN ID for a port. (Range: 1-4094, no leading zeroes)

DEFAULT SETTING

VLAN 1

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- When using Access mode, and an interface is assigned to a new VLAN, its PVID is automatically set to the identifier for that VLAN. When using Hybrid mode, the PVID for an interface can be set to any VLAN for which it is an untagged member.
- If acceptable frame types is set to **all** or switchport mode is set to **hybrid**, the PVID will be inserted into all untagged frames entering the ingress port.

EXAMPLE

The following example shows how to set the PVID for port 1 to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport native vlan 3
Console(config-if)#
```

vlan-trunking

This command allows unknown VLAN groups to pass through the specified interface. Use the **no** form to disable this feature.

SYNTAX

[**no**] **vlan-trunking**

DEFAULT SETTING

Disabled

COMMAND MODE

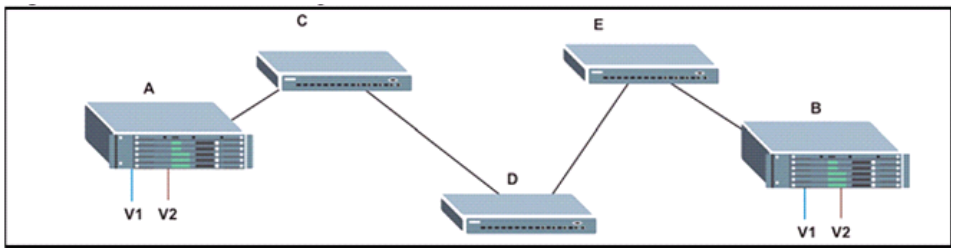
Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- Use this command to configure a tunnel across one or more intermediate switches which pass traffic for VLAN groups to which they do not belong.

  The following figure shows VLANs 1 and 2 configured on switches A and B, with VLAN trunking being used to pass traffic for these VLAN groups across switches C, D and E.

  Figure 218: Configuring VLAN Trunking

  Without VLAN trunking, you would have to configure VLANs 1 and 2 on all intermediate switches – C, D and E; otherwise these switches would drop any frames with unknown VLAN group tags. However, by enabling VLAN trunking on the intermediate switch ports along the path connecting VLANs 1 and 2, you only need to create these VLAN groups in switches A and B. Switches C, D and E automatically allow frames with VLAN group tags 1 and 2 (groups that are unknown to those switches) to pass through their VLAN trunking ports.

- VLAN trunking is mutually exclusive with the "access" switchport mode (see the switchport mode command). If VLAN trunking is enabled on an interface, then that interface cannot be set to access mode, and vice versa.

- To prevent loops from forming in the spanning tree, all unknown VLANs will be bound to a single instance (either STP/RSTP or an MSTP instance, depending on the selected STA mode).

- If both VLAN trunking and ingress filtering are disabled on an interface, packets with unknown VLAN tags will still be allowed to enter this interface and will be flooded to all other ports where VLAN trunking is enabled. (In other words, VLAN trunking will still be effectively enabled for the unknown VLAN).

EXAMPLE

The following example enables VLAN trunking on ports 9 and 10 to establish a path across the switch for unknown VLAN groups:

```
Console(config)#interface ethernet 1/9
Console(config-if)#vlan-trunking
Console(config-if)#interface ethernet 1/10
Console(config-if)#vlan-trunking
Console(config-if)#
```

DISPLAYING VLAN INFORMATION

This section describes commands used to display VLAN information.

Table 116: Commands for Displaying VLAN Information

Command	Function	Mode
show interfaces status vlan	Displays status for the specified VLAN interface	NE, PE
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE
show vlan	Shows VLAN information	NE, PE

show vlan

This command shows VLAN information.

SYNTAX

show vlan [**id** *vlan-id* | **name** *vlan-name* | **private-vlan** *private-vlan-type*]

id - Keyword to be followed by the VLAN ID.

vlan-id - ID of the configured VLAN. (Range: 1-4094, no leading zeroes)

name - Keyword to be followed by the VLAN name.

vlan-name - ASCII string from 1 to 32 characters.

private-vlan - For an explanation of this command see the show vlan private-vlan command.

private-vlan-type - Indicates the private VLAN type. (Options: community, primary)

DEFAULT SETTING

Shows all VLANs.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

The following example shows how to display information for VLAN 1:

```
Console#show vlan id 1
Default VLAN ID : 1


VLAN ID:               1
Type:                  Static
Name:                  DefaultVlan
Status:                Active
Ports/Port Channels:   Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
                       Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
                       Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S)
                       Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S) Eth1/20(S)
```

```
                                Eth1/21(S) Eth1/22(S) Eth1/23(S) Eth1/24(S) Eth1/25(S)
                                Eth1/26(S) Eth1/27(S) Eth1/28(S)

Console#
```

CONFIGURING IEEE 802.1Q TUNNELING

IEEE 802.1Q tunneling (QinQ tunneling) uses a single Service Provider VLAN (SPVLAN) for customers who have multiple VLANs. Customer VLAN IDs are preserved and traffic from different customers is segregated within the service provider's network even when they use the same customer-specific VLAN IDs. QinQ tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy, preserving the customer's original tagged packets, and adding SPVLAN tags to each frame (also called double tagging).

This section describes commands used to configure QinQ tunneling.

Table 117: 802.1Q Tunneling Commands

Command	Function	Mode
Basic 802.1Q Tunnel Commands		
dot1q-tunnel system-tunnel-control	Configures the switch to operate in normal mode or QinQ mode	GC
switchport dot1q-tunnel mode	Configures an interface as a QinQ tunnel port	IC
switchport dot1q-tunnel service match cvid	Creates a CVLAN to SPVLAN mapping entry	IC
switchport dot1q-tunnel tpid	Sets the Tag Protocol Identifier (TPID) value of a tunnel port	IC
show dot1q-tunnel	Displays the configuration of QinQ tunnel ports	PE
show interfaces switchport	Displays port QinQ operational status	PE
L2 Protocol Tunnel Commands		
l2protocol-tunnel tunnel-dmac	Configures the destination address for Layer 2 Protocol Tunneling	GC
switchport l2protocol-tunnel	Enables Layer 2 Protocol Tunneling for the specified protocol	IC
show l2protocol-tunnel	Shows settings for Layer 2 Protocol Tunneling	PE

General Configuration Guidelines for QinQ

1. Configure the switch to QinQ mode (dot1q-tunnel system-tunnel-control).
2. Create a SPVLAN (vlan).
3. Configure the QinQ tunnel access port to dot1Q-tunnel access mode (switchport dot1q-tunnel mode).

4. Set the Tag Protocol Identifier (TPID) value of the tunnel access port. This step is required if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The standard ethertype value is 0x8100. (See switchport dot1q-tunnel tpid.)

5. Configure the QinQ tunnel access port to join the SPVLAN as an untagged member (switchport allowed vlan).

6. Configure the SPVLAN ID as the native VID on the QinQ tunnel access port (switchport native vlan).

7. Configure the QinQ tunnel uplink port to dot1Q-tunnel uplink mode (switchport dot1q-tunnel mode).

8. Configure the QinQ tunnel uplink port to join the SPVLAN as a tagged member (switchport allowed vlan).

Limitations for QinQ

- The native VLAN for the tunnel uplink ports and tunnel access ports cannot be the same. However, the same service VLANs can be set on both tunnel port types.
- IGMP Snooping should not be enabled on a tunnel access port.
- If the spanning tree protocol is enabled, be aware that a tunnel access or tunnel uplink port may be disabled if the spanning tree structure is automatically reconfigured to overcome a break in the tree. It is therefore advisable to disable spanning tree on these ports.

dot1q-tunnel system-tunnel-control

This command sets the switch to operate in QinQ mode. Use the **no** form to disable QinQ operating mode.

SYNTAX

[**no**] **dot1q-tunnel system-tunnel-control**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

QinQ tunnel mode must be enabled on the switch for QinQ interface settings to be functional.

EXAMPLE

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#
```

RELATED COMMANDS

show dot1q-tunnel (818)
show interfaces switchport (695)

switchport dot1q-tunnel mode

This command configures an interface as a QinQ tunnel port. Use the **no** form to disable QinQ on the interface.

SYNTAX

switchport dot1q-tunnel mode {**access** | **uplink**}

no switchport dot1q-tunnel mode

access – Sets the port as an 802.1Q tunnel access port.

uplink – Sets the port as an 802.1Q tunnel uplink port.

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- QinQ tunneling must be enabled on the switch using the dot1q-tunnel system-tunnel-control command before the **switchport dot1q-tunnel mode** interface command can take effect.
- When a tunnel uplink port receives a packet from a customer, the customer tag (regardless of whether there are one or more tag layers) is retained in the inner tag, and the service provider's tag added to the outer tag.
- When a tunnel uplink port receives a packet from the service provider, the outer service provider's tag is stripped off, and the packet passed on to the VLAN indicated by the inner tag. If no inner tag is found, the packet is passed onto the native VLAN defined for the uplink port.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#
```

RELATED COMMANDS

show dot1q-tunnel (818)
show interfaces switchport (695)

switchport dot1q-tunnel service match cvid

This command creates a CVLAN to SPVLAN mapping entry. Use the **no** form to delete a VLAN mapping entry.

SYNTAX

switchport dot1q-tunnel service *outer-vlan* **match cvid** *inner-vlan*

outer-vlan - VLAN ID for the outer VLAN tag (SPVID). (Range: 1-4094, no leading zeroes)

inner-vlan - VLAN ID for the inner VLAN tag (CVID). (Range: 1-4094, no leading zeroes)

DEFAULT SETTING

Default mapping uses the PVID of the ingress port on the edge router for the SPVID.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- The inner VLAN tag of a customer packet entering the edge router of a service provider's network is mapped to an outer tag indicating the service provider VLAN that will carry this traffic across the 802.1Q tunnel. By default, the outer tag is based on the default VID of the edge router's ingress port. This process is performed in a transparent manner as described under "IEEE 802.1Q Tunneling" on page 339.

- When priority bits are found in the inner tag, these are also copied to the outer tag. This allows the service provider to differentiate service based on the indicated priority and appropriate methods of queue management at intermediate nodes across the tunnel.

- Rather than relying on standard service paths and priority queuing, QinQ VLAN mapping can be used to further enhance service by defining a set of differentiated service pathways to follow across the service provider's network for traffic arriving from specified inbound customer VLANs.

- Note that all interfaces are configured as uplink interfaces by default (that is, a network-to-network interface). Using the switchport dot1q-tunnel mode access command configures an interface as access interface (that is, a user-to-network interface).

EXAMPLE

This example sets the SVID to 99 in the outer tag for egress packets exiting port 1 when the packet's CVID is 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel service 99 match cvid 2
Console(config-if)#
```

switchport dot1q-tunnel tpid

This command sets the Tag Protocol Identifier (TPID) value of a tunnel port. Use the **no** form to restore the default setting.

SYNTAX

switchport dot1q-tunnel tpid *tpid*

no switchport dot1q-tunnel tpid

tpid – Sets the ethertype value for 802.1Q encapsulation. This identifier is used to select a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The standard ethertype value is 0x8100. (Range: 0800-FFFF hexadecimal)

DEFAULT SETTING

0x8100

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- Use the **switchport dot1q-tunnel tpid** command to set a custom 802.1Q ethertype value on the selected interface. This feature allows the switch to interoperate with third-party switches that do not use the standard 0x8100 ethertype to identify 802.1Q-tagged frames. For example, 0x1234 is set as the custom 802.1Q ethertype on a trunk port, incoming frames containing that ethertype are assigned to the VLAN contained in the tag following the ethertype field, as they would be with a standard 802.1Q trunk. Frames arriving on the port containing any other ethertype are looked upon as untagged frames, and assigned to the native VLAN of that port.

- All ports on the switch will be set to the same ethertype.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel tpid 9100
Console(config-if)#
```

RELATED COMMANDS

show interfaces switchport (695)

show dot1q-tunnel

This command displays information about QinQ tunnel ports.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
```

```
Console(config-if)#interface ethernet 1/2
Console(config-if)#switchport dot1q-tunnel mode uplink
Console(config-if)#end
Console#show dot1q-tunnel

Current double-tagged status of the system is Enabled
The dot1q-tunnel mode of the set interface 1/1 is Access mode, TPID is 0x8100.
The dot1q-tunnel mode of the set interface 1/2 is Uplink mode, TPID is 0x8100.
The dot1q-tunnel mode of the set interface 1/3 is Normal mode, TPID is 0x8100.
.
.
.
```

RELATED COMMANDS

switchport dot1q-tunnel mode (816)

l2protocol-tunnel tunnel-dmac

This command configures the destination address for Layer 2 Protocol Tunneling (L2PT). Use the **no** form to restore the default setting.

SYNTAX

l2protocol-tunnel tunnel-dmac *mac-address*

mac-address – The switch rewrites the destination MAC address in all upstream L2PT protocol packets (i.e, STP BPDUs) to this value, and forwards them on to uplink ports. The MAC address must be specified in the format xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.

DEFAULT SETTING

01-12-CF-.00-00-02, proprietary tunnel address

COMMAND MODE

Global Configuration

COMMAND USAGE

- When L2PT is not used, spanning tree protocol packets are flooded to 802.1Q access ports on the same edge switch, but filtered from 802.1Q tunnel ports. This creates disconnected protocol domains in the customer's network.
- L2PT can be used to pass BPDU packets belonging to the same customer transparently across a service provider's network. In this way, normally segregated network segments can be configured to function inside a common protocol domain.
- L2PT encapsulates protocol packets entering ingress ports on the service provider's edge switch, replacing the destination MAC address with a proprietary MAC address for the spanning tree protocol (i.e., 10-12-CF-00-00-02) or a user-defined address. All intermediate switches carrying this traffic across the service provider's network treat these encapsulated packets in the same way as normal data, forwarding them across to the tunnel's egress port. The egress port decapsulates these packets, restores the proper protocol and MAC address information, and then floods them onto the same VLANs at the

customer's remote site (via all of the appropriate tunnel ports and access ports[23] connected to the same metro VLAN).

- For L2PT to function properly, QinQ must be enabled on the switch using the dot1q-tunnel system-tunnel-control command, and the interface configured to 802.1Q tunnel mode using the switchport dot1q-tunnel mode command.

EXAMPLE

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#l2protocol-tunnel tunnel-dmac 01-80-C2-00-00-01
Console(config-)#
```

switchport l2protocol-tunnel

This command enables Layer 2 Protocol Tunneling (L2PT) for the specified protocol. Use the **no** form to disable L2PT for the specified protocol.

SYNTAX

switchport l2protocol-tunnel spanning-tree

spanning-tree - Spanning Tree (STP, RSTP, MSTP, PVST+)

DEFAULT SETTING

Disabled for all protocols

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- Refer to the Command Usage section for the l2protocol-tunnel tunnel-dmac command.

- For L2PT to function properly, QinQ must be enabled on the switch using the dot1q-tunnel system-tunnel-control command, and the interface configured to 802.1Q tunnel mode using the switchport dot1q-tunnel mode command.

EXAMPLE

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#switchport l2protocol-tunnel spanning-tree
Console(config-if)#
```

23. Access ports in this context are 802.1Q trunk ports.

show l2protocol-tunnel

This command shows settings for Layer 2 Protocol Tunneling (L2PT).

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show l2protocol-tunnel
Layer 2 Protocol Tunnel

Interface  Protocol
------------------------------------------------------------
Eth 1/ 1   Spanning Tree
Console#
```

CONFIGURING PORT-BASED TRAFFIC SEGMENTATION

If tighter security is required for passing traffic from different clients through downlink ports on the local network and over uplink ports to the service provider, port-based traffic segmentation can be used to isolate traffic for individual clients.

Traffic belonging to each client is isolated to the allocated downlink ports. But the switch can be configured to either isolate traffic passing across a client's allocated uplink ports from the uplink ports assigned to other clients, or to forward traffic through the uplink ports used by other clients, allowing different clients to share access to their uplink ports where security is less likely to be compromised.

Table 118: Traffic Segmentation Commands

Command	Function	Mode
pvlan	Enables traffic segmentation	GC
pvlan uplink/downlink	Configures uplink/downlink ports for client sessions	GC
pvlan session	Creates a client session	GC
pvlan up-to-up	Specifies whether or not traffic can be forwarded between uplink ports assigned to different client sessions	GC
show pvlan	Displays the traffic segmentation configuration settings	PE

pvlan

This command enables port-based traffic segmentation. Use the **no** form to disable this feature.

SYNTAX

[**no**] **pvlan**

DEFAULT SETTING

Disabled

COMMAND MODE
Global Configuration

COMMAND USAGE
- When traffic segmentation is enabled, the forwarding state for the uplink and downlink ports assigned to different client sessions is shown below.

Table 119: Traffic Segmentation Forwarding

Destination Source	Session #1 Downlinks	Session #1 Uplinks	Session #2 Downlinks	Session #2 Downlinks	Normal Ports
Session #1 Downlink Ports	Blocking	Forwarding	Blocking	Blocking	Blocking
Session #1 Uplink Ports	Forwarding	Forwarding	Blocking	Blocking/ Forwarding*	Forwarding
Session #2 Downlink Ports	Blocking	Blocking	Blocking	Forwarding	Blocking
Session #2 Uplink Ports	Blocking	Blocking/ Forwarding*	Forwarding	Forwarding	Forwarding
Normal Ports	Forwarding	Forwarding	Forwarding	Forwarding	Forwarding

* The forwarding state for uplink-to-uplink ports is configured by the pvlan uplink/ downlink command.

- When traffic segmentation is disabled, all ports operate in normal forwarding mode based on the settings specified by other functions such as VLANs and spanning tree protocol.

EXAMPLE

```
Console(config)#pvlan
Console(config)#
```

pvlan uplink/ downlink

This command configures uplink/downlink ports for traffic-segmentation client sessions. Use the **no** form to restore a port to normal operating mode.

SYNTAX

[**no**] **pvlan** [**session** *session-id*] {**uplink** *interface-list* [**downlink** *interface-list*] | **downlink** *interface-list*}

session-id – Traffic segmentation session. (Range: 1-15)

interface-list – One or more uplink or downlink interfaces.

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING
None

COMMAND MODE
Global Configuration

COMMAND USAGE
- A port cannot be configured in both an uplink and downlink list.
- A port can only be assigned to one traffic-segmentation session.
- A downlink port can only communicate with an uplink port in the same session. Therefore, if an uplink port is not configured for a session, the assigned downlink ports will not be able to communicate with any other ports.
- If a downlink port is not configured for the session, the assigned uplink ports will operate as normal ports.
- Due to switch ASIC limitations, ports 1-8, 9-16, 17-24 on the ES3528M and ports 1-24, 25-48 on the ES3552M are grouped together when any group member is configured as an uplink or downlink interface.

EXAMPLE

```
Console(config)#pvlan session 1 uplink ethernet 1/25 downlink ethernet 1/1
Console(config)#
```

pvlan session

This command creates a traffic-segmentation client session. Use the **no** form to remove a client session.

SYNTAX

[**no**] **pvlan session** *session-id*

session-id – Traffic segmentation session. (Range: 1-15)

DEFAULT SETTING
None

COMMAND MODE
Global Configuration

COMMAND USAGE
- Use this command to create a new traffic-segmentation client session.
- Using the **no** form of this command will remove any assigned uplink or downlink ports, restoring these interfaces to normal operating mode.

EXAMPLE

```
Console(config)#pvlan session 1
Console(config)#
```

pvlan up-to-up

This command specifies whether or not traffic can be forwarded between uplink ports assigned to different client sessions. Use the **no** form to restore the default.

SYNTAX

[**no**] **pvlan up-to-up** {**blocking** | **forwarding**}

blocking – Blocks traffic between uplink ports assigned to different sessions.

forwarding – Forwards traffic between uplink ports assigned to different sessions.

DEFAULT SETTING

Blocking

COMMAND MODE

Global Configuration

EXAMPLE

This example enables forwarding of traffic between uplink ports assigned to different client sessions.

```
Console(config)#pvlan up-to-up forwarding
Console(config)#
```

show pvlan

This command displays the traffic segmentation configuration settings.

SYNTAX

show pvlan [**session** *session-id*]

session-id – Traffic segmentation session. (Range: 1-15)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show pvlan

 Private VLAN Status   :                 Enabled
 Uplink-to-Uplink Mode :                 Forwarding
```

```
 Session   Uplink Ports                    Downlink Ports
--------- ------------------------------ ------------------------------
    1      Ethernet  1/25                 Ethernet  1/1
                                          Ethernet  1/2
                                          Ethernet  1/3
                                          Ethernet  1/4
                                          Ethernet  1/5
                                          Ethernet  1/6
                                          Ethernet  1/7
                                          Ethernet  1/8

Console#
```

CONFIGURING PRIVATE VLANS

Private VLANs provide port-based security and isolation of local ports contained within different private VLAN groups. This switch supports two types of private VLANs – primary and community groups. A primary VLAN contains promiscuous ports that can communicate with all other ports in the associated private VLAN groups, while a community (or secondary) VLAN contains community ports that can only communicate with other hosts within the community VLAN and with any of the promiscuous ports in the associated primary VLAN. The promiscuous ports are designed to provide open access to an external network such as the Internet, while the community ports provide restricted access to local users.

Multiple primary VLANs can be configured on this switch, and multiple community VLANs can be associated with each primary VLAN. (Note that private VLANs and normal VLANs can exist simultaneously within the same switch.)

This section describes commands used to configure private VLANs.

Table 120: Private VLAN Commands

Command	Function	Mode
Edit Private VLAN Groups		
private-vlan	Adds or deletes primary or community VLANs	VC
private vlan association	Associates a community VLAN with a primary VLAN	VC
Configure Private VLAN Interfaces		
switchport mode private-vlan	Sets an interface to host mode or promiscuous mode	IC
switchport private-vlan host-association	Associates an interface with a secondary VLAN	IC
switchport private-vlan mapping	Maps an interface to a primary VLAN	IC
Display Private VLAN Information		
show vlan private-vlan	Shows private VLAN information	NE, PE

To configure private VLANs, follow these steps:

1. Use the private-vlan command to designate one or more community VLANs and the primary VLAN that will channel traffic outside of the community groups.
2. Use the private vlan association command to map the community VLAN(s) to the primary VLAN.
3. Use the switchport mode private-vlan command to configure ports as promiscuous (i.e., having access to all ports in the primary VLAN) or host (i.e., community port).
4. Use the switchport private-vlan host-association command to assign a port to a community VLAN.
5. Use the switchport private-vlan mapping command to assign a port to a primary VLAN.
6. Use the show vlan private-vlan command to verify your configuration settings.

private-vlan

Use this command to create a primary or community private VLAN. Use the **no** form to remove the specified private VLAN.

SYNTAX

private-vlan *vlan-id* {**community** | **primary**}

no private-vlan *vlan-id*

vlan-id - ID of private VLAN. (Range: 2-4094, no leading zeroes).

community - A VLAN in which traffic is restricted to host members in the same VLAN and to promiscuous ports in the associate primary VLAN.

primary - A VLAN which can contain one or more community VLANs, and serves to channel traffic between community VLANs and other locations.

DEFAULT SETTING

None

COMMAND MODE

VLAN Configuration

COMMAND USAGE

- Private VLANs are used to restrict traffic to ports within the same community, and channel traffic passing outside the community through promiscuous ports. When using community VLANs, they must be mapped to an associated "primary" VLAN that contains promiscuous ports.

- Port membership for private VLANs is static. Once a port has been assigned to a private VLAN, it cannot be dynamically moved to another VLAN via GVRP.
- Private VLAN ports cannot be set to trunked mode. (See the switchport mode command.)

EXAMPLE

```
Console(config)#vlan database
Console(config-vlan)#private-vlan 2 primary
Console(config-vlan)#private-vlan 3 community
Console(config)#
```

private vlan association

Use this command to associate a primary VLAN with a secondary (i.e., community) VLAN. Use the **no** form to remove all associations for the specified primary VLAN.

SYNTAX

private-vlan *primary-vlan-id* **association** {*secondary-vlan-id* | **add** *secondary-vlan-id* | **remove** *secondary-vlan-id*}

no private-vlan *primary-vlan-id* **association**

primary-vlan-id - ID of primary VLAN. (Range: 2-4094, no leading zeroes).

secondary-vlan-id - ID of secondary (i.e, community) VLAN. (Range: 2-4094, no leading zeroes).

DEFAULT SETTING

None

COMMAND MODE

VLAN Configuration

COMMAND USAGE

Secondary VLANs provide security for group members. The associated primary VLAN provides a common interface for access to other network resources within the primary VLAN (e.g., servers configured with promiscuous ports) and to resources outside of the primary VLAN (via promiscuous ports).

EXAMPLE

```
Console(config-vlan)#private-vlan 2 association 3
Console(config)#
```

switchport mode private-vlan

Use this command to set the private VLAN mode for an interface. Use the **no** form to restore the default setting.

SYNTAX

switchport mode private-vlan {**host** | **promiscuous**}

no switchport mode private-vlan

host – This port type can subsequently be assigned to a community VLAN.

promiscuous – This port type can communicate with all other promiscuous ports in the same primary VLAN, as well as with all the ports in the associated secondary VLANs.

DEFAULT SETTING

Normal VLAN

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

To assign a promiscuous port to a primary VLAN, use the switchport private-vlan mapping command. To assign a host port to a community VLAN, use the switchport private-vlan host-association command.

EXAMPLE

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport mode private-vlan promiscuous
Console(config-if)#exit
Console(config)#interface ethernet 1/3
Console(config-if)#switchport mode private-vlan host
Console(config-if)#
```

switchport private-vlan host-association

Use this command to associate an interface with a secondary VLAN. Use the **no** form to remove this association.

SYNTAX

switchport private-vlan host-association *secondary-vlan-id*

no switchport private-vlan host-association

secondary-vlan-id - ID of secondary (i.e., community) VLAN. (Range: 1-4094, no leading zeroes).

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

All ports assigned to a secondary (i.e., community) VLAN can pass traffic between group members, but must communicate with resources outside of the group via promiscuous ports in the associated primary VLAN.

EXAMPLE

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport private-vlan host-association 3
Console(config-if)#
```

switchport private-vlan mapping

Use this command to map an interface to a primary VLAN. Use the **no** form to remove this mapping.

SYNTAX

switchport private-vlan mapping *primary-vlan-id*

no switchport private-vlan mapping

primary-vlan-id – ID of primary VLAN. (Range: 1-4094, no leading zeroes).

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

Promiscuous ports assigned to a primary VLAN can communicate with any other promiscuous ports in the same VLAN, and with the group members within any associated secondary VLANs.

EXAMPLE

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport private-vlan mapping 2
Console(config-if)#
```

show vlan private-vlan

Use this command to show the private VLAN configuration settings on this switch.

SYNTAX

show vlan private-vlan [**community** | **primary**]

community – Displays all community VLANs, along with their associated primary VLAN and assigned host interfaces.

primary – Displays all primary VLANs, along with any assigned promiscuous interfaces.

DEFAULT SETTING
None

COMMAND MODE
Privileged Executive

EXAMPLE

```
Console#show vlan private-vlan
Primary   Secondary       Type       Interfaces
--------  -----------  ----------  ------------------------------
     5                 primary     Eth1/ 3
     5         6       community   Eth1/ 4 Eth1/ 5
Console#
```

CONFIGURING PROTOCOL-BASED VLANS

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type in use by the inbound packets.

.

Table 121: Protocol-based VLAN Commands

Command	Function	Mode
protocol-vlan protocol-group	Create a protocol group, specifying the supported protocols	GC
protocol-vlan protocol-group	Maps a protocol group to a VLAN	IC
show protocol-vlan protocol-group	Shows the configuration of protocol groups	PE
show protocol-vlan protocol-group-vid	Shows the mapping of protocol groups to VLAN	PE

To configure protocol-based VLANs, follow these steps:

1. First configure VLAN groups for the protocols you want to use (page 805). Although not mandatory, we suggest configuring a separate VLAN for each major protocol running on your network. Do not add port members at this time.

2. Create a protocol group for each of the protocols you want to assign to a VLAN using the protocol-vlan protocol-group add command (Global Configuration mode).

3. Then map the protocol for each interface to the appropriate VLAN using the protocol-vlan protocol-group vlan command (Interface Configuration mode).

NOTE: Traffic which matches IP Protocol Ethernet Frames is mapped to the VLAN (VLAN 1) that has been configured with the switch's administrative IP. IP Protocol Ethernet traffic must not be mapped to another VLAN or you will lose administrative network connectivity to the switch. If lost in this manner, network access can be regained by removing the offending Protocol VLAN rule via the console. Alternately, the switch can be power-cycled, however all unsaved configuration changes will be lost.

protocol-vlan protocol-group (Configuring Groups)

This command creates a protocol group, or adds specific protocols to a group. Only one frame type and protocol type can be added to a protocol group. Use the **no** form to remove a protocol group.

SYNTAX

protocol-vlan protocol-group *group-id* [{**add** | **remove**} **frame-type** *frame* **protocol-type** *protocol*]

no protocol-vlan protocol-group *group-id*

group-id - Group identifier of this protocol group. (Range: 1-2147483647)

frame[24] - Frame type used by this protocol. (Options: ethernet, rfc_1042, llc_other)

protocol - Protocol type. The protocols supported each frame type includes:

ethernet - arp, ip, pppoe, rarp

llc-other - ipx-raw

rfc-1042 - arp, ip, rarp.

DEFAULT SETTING

No protocol groups are configured.

COMMAND MODE

Global Configuration

24. SNAP frame types are not supported by this switch due to hardware limitations.

EXAMPLE

The following creates protocol group 1, and specifies Ethernet frames with IP and ARP protocol types:

```
Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet
  protocol-type ip
Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet
  protocol-type arp
Console(config)#
```

protocol-vlan protocol-group (Configuring Interfaces)

This command maps a protocol group entering any interface to a VLAN. Use the **no** form to remove the protocol mapping.

SYNTAX

protocol-vlan protocol-group *group-id* **vlan** *vlan-id*

no protocol-vlan protocol-group *group-id* **vlan**

group-id - Group identifier of this protocol group. (Range: 1-2147483647)

vlan-id - VLAN to which matching protocol traffic is forwarded. (Range: 1-4094)

DEFAULT SETTING

No protocol groups are mapped for any VLAN.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- When creating a protocol-based VLAN, only assign interfaces via this command. If you assign interfaces using any of the other VLAN commands (such as the vlan command), the switch will admit traffic of any protocol type into the associated VLAN.
- A maximum of 20 protocol VLAN groups can be defined on the switch.
- When a frame enters the switch and protocol VLANs have been configured, the frame is processed in the following manner:
  - If the frame is tagged, it will be processed according to the standard rules applied to tagged frames.
  - If the frame is untagged and the protocol type matches, the frame is forwarded to the appropriate VLAN.
  - If the frame is untagged but the protocol type does not match, the frame is forwarded to the default VLAN for this interface.

EXAMPLE

The following example maps the traffic matching the protocol type specified in protocol group 1 to VLAN 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan 2
Console(config-if)#
```

show protocol-vlan protocol-group

This command shows the frame and protocol type associated with protocol groups.

SYNTAX

show protocol-vlan protocol-group [*group-id*]

group-id - Group identifier for a protocol group. (Range: 1-2147483647)

DEFAULT SETTING

All protocol groups are displayed.

COMMAND MODE

Privileged Exec

EXAMPLE

This shows protocol group 1 configured for IP over Ethernet:

```
Console#show protocol-vlan protocol-group

 Protocol Group ID   Frame Type    Protocol Type
------------------ ------------- ---------------
                 1      ethernet     08 00
Console#
```

show protocol-vlan protocol-group-vid

This command shows the mapping from protocol groups to VLANs.

SYNTAX

show interfaces protocol-vlan protocol-group-vid

DEFAULT SETTING

The mapping for all interfaces is displayed.

COMMAND MODE

Privileged Exec

EXAMPLE

This shows that traffic matching the specifications for protocol group 1 will be mapped to VLAN 2:

```
Console#show interfaces protocol-vlan protocol-group

ProtocolGroup ID    VLAN ID
----------------- -----------
              1       VLAN2
Console#
```

CONFIGURING IP SUBNET VLANS

When using IEEE 802.1Q port-based VLAN classification, all untagged frames received by a port are classified as belonging to the VLAN whose VID (PVID) is associated with that port.

When IP subnet-based VLAN classification is enabled, the source address of untagged ingress frames are checked against the IP subnet-to-VLAN mapping table. If an entry is found for that subnet, these frames are assigned to the VLAN indicated in the entry. If no IP subnet is matched, the untagged frames are classified as belonging to the receiving port's VLAN ID (PVID).

Table 122: IP Subnet VLAN Commands

Command	Function	Mode
subnet-vlan	Defines the IP Subnet VLANs	GC
show subnet-vlan	Displays IP Subnet VLAN settings	PE

subnet-vlan

This command configures IP Subnet VLAN assignments. Use the **no** form to remove an IP subnet-to-VLAN assignment.

SYNTAX

subnet-vlan subnet *ip-address mask* **vlan** *vlan-id*

no subnet-vlan subnet {*ip-address mask* | **all**}

ip-address – The IP address that defines the subnet. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.

mask – This mask identifies the host address bits of the IP subnet.

vlan-id – VLAN to which matching IP subnet traffic is forwarded. (Range: 1-4094)

DEFAULT SETTING

None

COMMAND MODE
Global Configuration

COMMAND USAGE
- Each IP subnet can be mapped to only one VLAN ID. An IP subnet consists of an IP address and a subnet mask.
- When an untagged frame is received by a port, the source IP address is checked against the IP subnet-to-VLAN mapping table, and if an entry is found, the corresponding VLAN ID is assigned to the frame. If no mapping is found, the PVID of the receiving port is assigned to the frame.
- The IP subnet cannot be a broadcast or multicast IP address.
- When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

EXAMPLE
The following example assigns traffic for the subnet 192.168.12.192, mask 255.255.255.224, to VLAN 4.

```
Console(config)#subnet-vlan subnet 192.168.12.192 255.255.255.224 vlan 4
Console(config)#
```

show subnet-vlan

This command displays IP Subnet VLAN assignments.

COMMAND MODE
Privileged Exec

COMMAND USAGE
- Use this command to display subnet-to-VLAN mappings.
- The last matched entry is used if more than one entry can be matched.

EXAMPLE
The following example displays all configured IP subnet-based VLANs.

```
Console#show subnet-vlan
    IP address           Mask        VLAN ID
---------------- ----------------- ---------
 192.168.12.0      255.255.255.128         2
 192.168.12.128    255.255.255.192         3
 192.168.12.192    255.255.255.224         4
 192.168.12.224    255.255.255.240         5
 192.168.12.240    255.255.255.248         6
 192.168.12.248    255.255.255.252         7
 192.168.12.252    255.255.255.254         8
 192.168.12.254    255.255.255.255         9
```

```
 192.168.12.255    255.255.255.255        10
Console#
```

CONFIGURING MAC BASED VLANS

When using IEEE 802.1Q port-based VLAN classification, all untagged frames received by a port are classified as belonging to the VLAN whose VID (PVID) is associated with that port.

When MAC-based VLAN classification is enabled, the source address of untagged ingress frames are checked against the MAC address-to-VLAN mapping table. If an entry is found for that address, these frames are assigned to the VLAN indicated in the entry. If no MAC address is matched, the untagged frames are classified as belonging to the receiving port's VLAN ID (PVID).

Table 123: MAC Based VLAN Commands

Command	Function	Mode
mac-vlan	Defines the IP Subnet VLANs	GC
show mac-vlan	Displays IP Subnet VLAN settings	PE

mac-vlan

This command configures MAC address-to-VLAN mapping. Use the **no** form to remove an assignment.

SYNTAX

mac-vlan mac-address *mac-address* **vlan** *vlan-id*

no mac-vlan mac-address {*mac-address* | **all**}

mac-address – The source MAC address to be matched. Configured MAC addresses can only be unicast addresses. The MAC address must be specified in the format xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.

vlan-id – VLAN to which the matching source MAC address traffic is forwarded. (Range: 1-4094)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- The MAC-to-VLAN mapping applies to all ports on the switch.
- Source MAC addresses can be mapped to only one VLAN ID.
- Configured MAC addresses cannot be broadcast or multicast addresses.

- When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

EXAMPLE

The following example assigns traffic from source MAC address 00-00-00-11-22-33 to VLAN 10.

```
Console(config)#mac-vlan mac-address 00-00-00-11-22-33 vlan 10
Console(config)#
```

show mac-vlan

This command displays MAC address-to-VLAN assignments.

COMMAND MODE

Privileged Exec

COMMAND USAGE

Use this command to display MAC address-to-VLAN mappings.

EXAMPLE

The following example displays all configured MAC address-based VLANs.

```
Console#show mac-vlan
    MAC address       VLAN ID
------------------- ---------
 00-00-00-11-22-33         10
Console#
```

CONFIGURING VOICE VLANS

The switch allows you to specify a Voice VLAN for the network and set a CoS priority for the VoIP traffic. VoIP traffic can be detected on switch ports by using the source MAC address of packets, or by using LLDP (IEEE 802.1AB) to discover connected VoIP devices. When VoIP traffic is detected on a configured port, the switch automatically assigns the port to the Voice VLAN. Alternatively, switch ports can be manually configured.

Table 124: Voice VLAN Commands

Command	Function	Mode
voice vlan	Defines the Voice VLAN ID	GC
voice vlan aging	Configures the aging time for Voice VLAN ports	GC
voice vlan mac-address	Configures VoIP device MAC addresses	GC
switchport voice vlan	Sets the Voice VLAN port mode	IC
switchport voice vlan priority	Sets the VoIP traffic priority for ports	IC

Table 124: Voice VLAN Commands (Continued)

Command	Function	Mode
switchport voice vlan rule	Sets the automatic VoIP traffic detection method for ports	IC
switchport voice vlan security	Enables Voice VLAN security on ports	IC
show voice vlan	Displays Voice VLAN settings	PE

voice vlan

This command enables VoIP traffic detection and defines the Voice VLAN ID. Use the **no** form to disable the Voice VLAN.

SYNTAX

voice vlan *voice-vlan-id*

no voice vlan

voice-vlan-id - Specifies the voice VLAN ID. (Range: 1-4094)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- When IP telephony is deployed in an enterprise network, it is recommended to isolate the Voice over IP (VoIP) network traffic from other data traffic. Traffic isolation helps prevent excessive packet delays, packet loss, and jitter, which results in higher voice quality. This is best achieved by assigning all VoIP traffic to a single VLAN.
- VoIP traffic can be detected on switch ports by using the source MAC address of packets, or by using LLDP (IEEE 802.1AB) to discover connected VoIP devices. When VoIP traffic is detected on a configured port, the switch automatically assigns the port as a tagged member of the Voice VLAN.
- Only one Voice VLAN is supported and it must already be created on the switch before it can be specified as the Voice VLAN.
- The Voice VLAN ID cannot be modified when the global auto-detection status is enabled (see the switchport voice vlan command.

EXAMPLE

The following example enables VoIP traffic detection and specifies the Voice VLAN ID as 1234.

```
Console(config)#voice vlan 1234
Console(config)#
```

voice vlan aging

This command sets the Voice VLAN ID time out. Use the **no** form to restore the default.

SYNTAX

voice vlan aging *minutes*

no voice vlan

minutes - Specifies the port Voice VLAN membership time out. (Range: 5-43200 minutes)

DEFAULT SETTING

1440 minutes

COMMAND MODE

Global Configuration

COMMAND USAGE

The Voice VLAN aging time is the time after which a port is removed from the Voice VLAN when VoIP traffic is no longer received on the port.

EXAMPLE

The following example configures the Voice VLAN aging time as 3000 minutes.

```
Console(config)#voice vlan aging 3000
Console(config)#
```

voice vlan mac-address

This command specifies MAC address ranges to add to the OUI Telephony list. Use the **no** form to remove an entry from the list.

SYNTAX

voice vlan mac-address *mac-address* **mask** *mask-address* [**description** *description*]

no voice vlan mac-address *mac-address* **mask** *mask-address*

mac-address - Defines a MAC address OUI that identifies VoIP devices in the network. (For example, 01-23-45-00-00-00)

mask-address - Identifies a range of MAC addresses. (Range: 80-00-00-00-00-00 to FF-FF-FF-FF-FF-FF)

description - User-defined text that identifies the VoIP devices. (Range: 1-32 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- VoIP devices attached to the switch can be identified by the manufacturer's Organizational Unique Identifier (OUI) in the source MAC address of received packets. OUI numbers are assigned to manufacturers and form the first three octets of device MAC addresses. The MAC OUI numbers for VoIP equipment can be configured on the switch so that traffic from these devices is recognized as VoIP.

- Selecting a mask of FF-FF-FF-00-00-00 identifies all devices with the same OUI (the first three octets). Other masks restrict the MAC address range. Selecting FF-FF-FF-FF-FF-FF specifies a single MAC address.

EXAMPLE

The following example adds a MAC OUI to the OUI Telephony list.

```
Console(config)#voice vlan mac-address 00-12-34-56-78-90 mask ff-ff-ff-00-00-
  00 description A new phone
Console(config)#
```

switchport voice vlan

This command specifies the Voice VLAN mode for ports. Use the **no** form to disable the Voice VLAN feature on the port.

SYNTAX

switchport voice vlan {**manual** | **auto**}

no switchport voice vlan

manual - The Voice VLAN feature is enabled on the port, but the port must be manually added to the Voice VLAN.

auto - The port will be added as a tagged member to the Voice VLAN when VoIP traffic is detected on the port.

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration

COMMAND USAGE

When auto is selected, you must select the method to use for detecting VoIP traffic, either OUI or 802.1AB (LLDP) using the switchport voice vlan rule command. When OUI is selected, be sure to configure the MAC address ranges in the Telephony OUI list using the voice vlan mac-address command.

EXAMPLE

The following example sets port 1 to Voice VLAN auto mode.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan auto
Console(config-if)#
```

switchport voice vlan priority

This command specifies a CoS priority for VoIP traffic on a port. Use the **no** form to restore the default priority on a port.

SYNTAX

switchport voice vlan priority *priority-value*

no switchport voice vlan priority

priority-value - The CoS priority value. (Range: 0-6)

DEFAULT SETTING

6

COMMAND MODE

Interface Configuration

COMMAND USAGE

Specifies a CoS priority to apply to the port VoIP traffic on the Voice VLAN. The priority of any received VoIP packet is overwritten with the new priority when the Voice VLAN feature is active for the port.

EXAMPLE

The following example sets the CoS priority to 5 on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan priority 5
Console(config-if)#
```

switchport voice vlan rule

This command selects a method for detecting VoIP traffic on a port. Use the **no** form to disable the detection method on the port.

SYNTAX

[**no**] **switchport voice vlan rule** {**oui** | **lldp**}

oui - Traffic from VoIP devices is detected by the Organizationally Unique Identifier (OUI) of the source MAC address.

lldp - Uses LLDP to discover VoIP devices attached to the port.

DEFAULT SETTING
OUI: Enabled
LLDP: Disabled

COMMAND MODE
Interface Configuration

COMMAND USAGE
- When OUI is selected, be sure to configure the MAC address ranges in the Telephony OUI list (see the voice vlan mac-address command. MAC address OUI numbers must be configured in the Telephony OUI list so that the switch recognizes the traffic as being from a VoIP device.
- LLDP checks that the "telephone bit" in the system capability TLV is turned on. See "LLDP Commands" on page 905 for more information on LLDP.

EXAMPLE
The following example enables the OUI method on port 1 for detecting VoIP traffic.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan rule oui
Console(config-if)#
```

switchport voice vlan security

This command enables security filtering for VoIP traffic on a port. Use the **no** form to disable filtering on a port.

SYNTAX
[**no**] **switchport voice vlan security**

DEFAULT SETTING
Disabled

COMMAND MODE
Interface Configuration

COMMAND USAGE
- Security filtering discards any non-VoIP packets received on the port that are tagged with the voice VLAN ID. VoIP traffic is identified by source MAC addresses configured in the Telephony OUI list, or through LLDP that discovers VoIP devices attached to the switch. Packets received from non-VoIP sources are dropped.
- When enabled, be sure the MAC address ranges for VoIP devices are configured in the Telephony OUI list (voice vlan mac-address).

EXAMPLE

The following example enables security filtering on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan security
Console(config-if)#
```

show voice vlan

This command displays the Voice VLAN settings on the switch and the OUI Telephony list.

SYNTAX

show voice vlan {**oui** | **status**}

oui - Displays the OUI Telephony list.

status - Displays the global and port Voice VLAN settings.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show voice vlan status
Global Voice VLAN Status
Voice VLAN Status     : Enabled
Voice VLAN ID         : 1234
Voice VLAN aging time : 1440 minutes

Voice VLAN Port Summary
Port     Mode     Security Rule      Priority
-------- -------- -------- --------- --------
Eth 1/ 1 Auto     Enabled  OUI              6
Eth 1/ 2 Disabled Disabled OUI              6
Eth 1/ 3 Manual   Enabled  OUI              5
Eth 1/ 4 Auto     Enabled  OUI              6
Eth 1/ 5 Disabled Disabled OUI              6
Eth 1/ 6 Disabled Disabled OUI              6
Eth 1/ 7 Disabled Disabled OUI              6
Eth 1/ 8 Disabled Disabled OUI              6
Eth 1/ 9 Disabled Disabled OUI              6
Eth 1/10 Disabled Disabled OUI              6

Console#show voice vlan oui
OUIAddress        Mask              Description
00-12-34-56-78-9A FF-FF-FF-00-00-00 old phones
00-11-22-33-44-55 FF-FF-FF-00-00-00 new phones
00-98-76-54-32-10 FF-FF-FF-FF-FF-FF Chris' phone

Console#
```

38 CLASS OF SERVICE COMMANDS

The commands described in this section allow you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with four priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, the relative weight of each queue, and the mapping of frame priority tags to the switch's priority queues can be configured.

Table 125: Priority Commands

Command Group	Function
Priority Commands (Layer 2)	Configures the queue mode, the default priority for untagged frames, and maps class of service tags to hardware queues
Priority Commands (Layer 3 and 4)	Maps IP DSCP tags to class of service values

PRIORITY COMMANDS (LAYER 2)

This section describes commands used to configure Layer 2 traffic priority on the switch.

Table 126: Priority Commands (Layer 2)

Command	Function	Mode
queue mode	Sets the queue mode to strict priority or Weighted Round-Robin (WRR)	GC
queue cos-map	Assigns class-of-service values to the priority queues	IC
switchport priority default	Sets a port priority for incoming untagged frames	IC
show interfaces switchport	Displays the administrative and operational status of an interface	PE
show queue bandwidth	Shows round-robin weights assigned to the priority queues	PE
show queue cos-map	Shows the class-of-service map	PE
show queue mode	Shows the current queue mode	PE

queue mode

This command sets the scheduling mode to strict priority or Weighted Round-Robin (WRR) for the class of service (CoS) priority queues. Use the **no** form to restore the default value.

SYNTAX

queue mode {**strict** | **wrr**}

no queue mode

strict - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues. This ensures that the highest priority packets are always serviced first, ahead of all other traffic.

wrr - Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights (1, 2, 4, 8 for queues 0 - 3), servicing each queue in a round-robin fashion.

DEFAULT SETTING

Weighted Round Robin

COMMAND MODE

Global Configuration

COMMAND USAGE

- Strict priority requires all traffic in a higher priority queue to be processed before lower priority queues are serviced.
- WRR uses a relative weight for each queue which determines the number of packets the switch transmits every time it services a queue before moving on to the next queue. Thus, a queue weighted 8 will be allowed to transmit up to 8 packets, after which the next lower priority queue will be serviced according to it's weighting. This prevents the head-of-line blocking that can occur with strict priority queuing.

EXAMPLE

The following example sets the queue mode to strict priority service mode:

```
Console(config)#queue mode strict
Console(config)#
```

queue cos-map

This command assigns class of service (CoS) values to the priority queues (i.e., hardware output queues 0 - 3). Use the **no** form set the CoS map to the default values.

SYNTAX

queue cos-map *queue-id* [*cos1 ... cosn*]
no queue cos-map

queue-id - The ID of the priority queue. (Range: 0-3, where 3 is the highest priority queue)

cos1 ... cosn - The CoS values that are mapped to the queue ID. It is a space-separated list of numbers. The CoS value is a number from 0 to 7, where 7 is the highest priority.

DEFAULT SETTING

This switch supports Class of Service by using four priority queues, with Weighted Round Robin queuing for each port. Eight separate traffic classes are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown below.

Table 127: Default CoS Values to Egress Queues

Queue	0	1	2	4
Priority	1,2	0,3	4,5	6,7

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- CoS values assigned at the ingress port are also used at the egress port.
- This command sets the CoS priority for all interfaces.

EXAMPLE

The following example shows how to change the CoS assignments to a one-to-one mapping:

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue cos-map 0 0
Console(config-if)#queue cos-map 1 1
Console(config-if)#queue cos-map 2 2
Console(config-if)#exit
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
 CoS Value:      0 1 2 3 4 5 6 7
 Priority Queue: 0 1 2 3 4 5 6 7
Console#
```

switchport priority default

This command sets a priority for incoming untagged frames. Use the **no** form to restore the default value.

SYNTAX

switchport priority default *default-priority-id*

no switchport priority default

default-priority-id - The priority number for untagged ingress traffic. The priority is a number from 0 to 7. Seven is the highest priority.

DEFAULT SETTING

The priority is not set, and the default value for untagged frames received on the interface is zero.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- The precedence for priority mapping is IP DSCP, and then default switchport priority.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- The switch provides four priority queues for each port. It can be configured to use strict priority queuing or weighted queuing using the queue mode command. Inbound frames that do not have VLAN tags are tagged with the input port's default ingress user priority, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in queue 1 of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

EXAMPLE

The following example shows how to set a default priority on port 3 to 5:

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport priority default 5
Console(config-if)#
```

RELATED COMMANDS

show interfaces switchport (695)

show queue bandwidth

This command displays the weighted round-robin (WRR) bandwidth allocation for the four priority queues.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show queue bandwidth
Queue ID  Weight
 --------  ------
    0         1
    1         2
    2         4
    3         8
Console#
```

show queue cos-map

This command shows the class of service priority map.

SYNTAX

show queue cos-map [*interface*]

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
 CoS Value:      0 1 2 3 4 5 6 7
 Priority Queue: 2 0 1 3 4 5 6 7
Console#
```

show queue mode

This command shows the current queue mode.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show queue mode

Queue Mode: wrr
Console#
```

PRIORITY COMMANDS (LAYER 3 AND 4)

This section describes commands used to configure Layer 3 and 4 traffic priority mapping on the switch.

Table 128: Priority Commands (Layer 3 and 4)

Command	Function	Mode
map ip dscp	Enables IP DSCP class of service mapping	GC
map ip dscp	Maps IP DSCP value to a class of service	IC
show map ip dscp	Shows the IP DSCP map	PE

map ip dscp (Global Configuration)

This command enables IP DSCP mapping (i.e., Differentiated Services Code Point mapping). Use the **no** form to disable IP DSCP mapping.

SYNTAX

[**no**] **map ip dscp**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

The precedence for priority mapping is IP DSCP, and default switchport priority.

EXAMPLE

The following example shows how to enable IP DSCP mapping globally:

```
Console(config)#map ip dscp
Console(config)#
```

map ip dscp (Interface Configuration)

This command sets IP DSCP priority (i.e., Differentiated Services Code Point priority). Use the **no** form to restore the default table.

SYNTAX

map ip dscp *dscp-value* **cos** *cos-value*
no map ip dscp

dscp-value - 8-bit DSCP value. (Range: 0-63)

cos-value - Class-of-Service value (Range: 0-7)

DEFAULT SETTING

The DSCP default values are defined in the following table. Note that all the DSCP values that are not specified are mapped to CoS value 0.

Table 129: IP DSCP to CoS Vales

IP DSCP Value	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- The precedence for priority mapping is IP DSCP, and default switchport priority.
- DSCP priority values are mapped to default Class of Service values according to recommendations in the IEEE 802.1p standard, and then subsequently mapped to the four hardware priority queues.
- This command sets the IP DSCP priority for all interfaces.

EXAMPLE

The following example shows how to map IP DSCP value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#
```

show map ip dscp

This command shows the IP DSCP priority map.

SYNTAX

show map ip dscp [*interface*]

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show map ip dscp ethernet 1/1
DSCP mapping status: disabled

 Port      DSCP COS
 --------- ---- ---
  Eth 1/ 1    0   0
  Eth 1/ 1    1   0
  Eth 1/ 1    2   0
  Eth 1/ 1    3   0
⋮
  Eth 1/ 1   61   7
  Eth 1/ 1   62   7
  Eth 1/ 1   63   7
Console#
```

39 QUALITY OF SERVICE COMMANDS

The commands described in this section are used to configure Differentiated Services (DiffServ) classification criteria and service policies. You can classify traffic based on access lists, IP Precedence or DSCP values, or VLANs. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet.

Table 130: Quality of Service Commands

Command	Function	Mode
class-map	Creates a class map for a type of traffic	GC
description	Specifies the description of a class map	CM
match	Defines the criteria used to classify traffic	CM
rename	Redefines the name of a class map	CM
policy-map	Creates a policy map for multiple interfaces	GC
description	Specifies the description of a policy map	PM
class	Defines a traffic classification for the policy to act on	PM
rename	Redefines the name of a policy map	PM
police	Defines an enforcer for classified traffic based on a metered flow rate	PM-C
set	Classifies IP traffic by setting a CoS, DSCP, or IP-precedence value in a packet	PM-C
service-policy	Applies a policy map defined by the policy-map command to the input of a particular interface	IC
show class-map	Displays the QoS class maps which define matching criteria used for classifying traffic	PE
show policy-map	Displays the QoS policy maps which define classification criteria for incoming traffic, and may include policers for bandwidth limitations	PE
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface	PE

To create a service policy for a specific category of ingress traffic, follow these steps:

1. Use the class-map command to designate a class name for a specific category of traffic, and enter the Class Map configuration mode.
2. Use the match command to select a specific type of traffic based on an access list, a DSCP or IP Precedence value, or a VLAN.
3. Set an ACL to enable filtering for the criteria specified in the match command.

4. Use the policy-map command to designate a policy name for a specific manner in which ingress traffic will be handled, and enter the Policy Map configuration mode.

5. Use the class command to identify the class map, and enter Policy Map Class configuration mode. A policy map can contain multiple class statements.

6. Use the set command to modify the QoS value for matching traffic class, and use the police command to monitor the average flow and burst rate, and drop any traffic that exceeds the specified rate, or just reduce the DSCP service level for traffic exceeding the specified rate.

7. Use the service-policy command to assign a policy map to a specific interface.

NOTE: You can configure up to 1024 rules per Class Map. You can also include multiple classes in a Policy Map.

NOTE: Create a Class Map before creating a Policy Map. Otherwise, you will not be able to specify a Class Map with the class command after entering Policy-Map Configuration mode.

class-map

This command creates a class map used for matching packets to the specified class, and enters Class Map configuration mode. Use the **no** form to delete a class map.

SYNTAX

[**no**] **class-map** *class-map-name* [**match-any**]

class-map-name - Name of the class map. (Range: 1-16 characters)

match-any - Match any condition within a class map.

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- First enter this command to designate a class map and enter the Class Map configuration mode. Then use match commands to specify the criteria for ingress traffic that will be classified under this class map.

- Up to 1024 match commands are permitted per class map, and for the overall system.

- One or more class maps can be assigned to a policy map (page 857). The policy map is then bound by a service policy to an interface (page 860). A service policy defines packet classification, service

tagging, and bandwidth policing. Once a policy map has been bound to an interface, no additional class maps may be added to the policy map, nor any changes made to the assigned class maps with the match or set commands.

EXAMPLE

This example creates a class map call "rd-class," and sets it to match packets marked for DSCP service value 3:

```
Console(config)#class-map rd-class match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```

RELATED COMMANDS

show class-map (861)

description

This command specifies the description of a class map or policy map.

SYNTAX

description *string*

string - Description of the class map or policy map. (Range: 1-64 characters)

COMMAND MODE

Class Map Configuration
Policy Map Configuration

EXAMPLE

```
Console(config)#class-map rd-class#1
Console(config-cmap)#description matches packets marked for DSCP service
  value 3
Console(config-cmap)#
```

match

This command defines the criteria used to classify traffic. Use the **no** form to delete the matching criteria.

SYNTAX

[**no**] **match** {**access-list** *acl-name* | **ip dscp** *dscp* | **ip precedence** *ip-precedence* | **vlan** *vlan*}

acl-name - Name of the access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs. (Range: 1-16 characters)

dscp - A Differentiated Service Code Point value. (Range: 0-63)

ip-precedence - An IP Precedence value. (Range: 0-7)

vlan - A VLAN. (Range:1-4094)

DEFAULT SETTING
None

COMMAND MODE
Class Map Configuration

COMMAND USAGE
- First enter the class-map command to designate a class map and enter the Class Map configuration mode. Then use **match** command to specify the fields within ingress packets that must match to qualify for this class map.
- If an ingress packet matches an ACL specified by this command, any deny rules included in the ACL will be ignored.
- If match criteria includes an IP ACL or IP priority rule, then a VLAN rule cannot be included in the same class map.
- If match criteria includes a MAC ACL or VLAN rule, then neither an IP ACL nor IP priority rule can be included in the same class map.
- Up to 1024 match entries can be included in a class map.

EXAMPLE
This example creates a class map called "rd-class#1," and sets it to match packets marked for DSCP service value 3.

```
Console(config)#class-map rd-class#1 match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```

This example creates a class map call "rd-class#2," and sets it to match packets marked for IP Precedence service value 5.

```
Console(config)#class-map rd-class#2 match-any
Console(config-cmap)#match ip precedence 5
Console(config-cmap)#
```

This example creates a class map call "rd-class#3," and sets it to match packets marked for VLAN 1.

```
Console(config)#class-map rd-class#3 match-any
Console(config-cmap)#match vlan 1
Console(config-cmap)#
```

rename

This command redefines the name of a class map or policy map.

SYNTAX

rename *map-name*

map-name - Name of the class map or policy map. (Range: 1-16 characters)

COMMAND MODE

Class Map Configuration
Policy Map Configuration

EXAMPLE

```
Console(config)#class-map rd-class#1
Console(config-cmap)#rename rd-class#9
Console(config-cmap)#
```

policy-map

This command creates a policy map that can be attached to multiple interfaces, and enters Policy Map configuration mode. Use the **no** form to delete a policy map.

SYNTAX

[**no**] **policy-map** *policy-map-name*

policy-map-name - Name of the policy map. (Range: 1-16 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- Use the **policy-map** command to specify the name of the policy map, and then use the class command to configure policies for traffic that matches the criteria defined in a class map.
- A policy map can contain multiple class statements that can be applied to the same interface with the service-policy command.
- Create a Class Map (page 857) before assigning it to a Policy Map.

EXAMPLE

This example creates a policy called "rd-policy," uses the class command to specify the previously defined "rd-class," uses the set command to classify the service that incoming packets will receive, and then uses the police command to limit the average bandwidth to 100,000 Kbps, the burst rate to 1522 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

class

This command defines a traffic classification upon which a policy can act, and enters Policy Map Class configuration mode. Use the **no** form to delete a class map.

SYNTAX

[**no**] **class** *class-map-name*

class-map-name - Name of the class map. (Range: 1-16 characters)

DEFAULT SETTING

None

COMMAND MODE

Policy Map Configuration

COMMAND USAGE

- Use the policy-map command to specify a policy map and enter Policy Map configuration mode. Then use the **class** command to enter Policy Map Class configuration mode. And finally, use the set and police commands to specify the match criteria, where the:
  - set command classifies the service that an IP packet will receive
  - police command defines the maximum throughput, burst rate, and response to non-conforming traffic.
- Up to 200 classes can be included in a policy map. can also include multiple classes in a Policy Map.

EXAMPLE

This example creates a policy called "rd-policy," uses the **class** command to specify the previously defined "rd-class," uses the set command to classify the service that incoming packets will receive, and then uses the police command to limit the average bandwidth to 100,000 Kbps, the burst

rate to 1522 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 10000 1522 exceed-action drop
Console(config-pmap-c)#
```

police

This command defines a policer for classified traffic based on the metered flow rate. Use the **no** form to remove a policer.

SYNTAX

[**no**] **police** *rate-kbps burst-byte* [**exceed-action** {**drop** | **set**}]

rate-kbps - Committed information rate in kilobits per second. (Range: 1-100000 kbps or maximum port speed, whichever is lower)

burst-byte - Committed burst size in bytes. (Range: 64-1522 bytes)

drop - Drop packet when specified rate or burst are exceeded.

set - Set DSCP service to the specified value. (Range: 0-63)

DEFAULT SETTING

Drop out-of-profile packets.

COMMAND MODE

Policy Map Class Configuration

COMMAND USAGE

- You can configure up to 64 policers (i.e., meters or class maps) for each of the following access list types: MAC ACL, IP ACL (including Standard ACL and Extended ACL), IPv6 Standard ACL, and IPv6 Extended ACL.
- Policing is based on a token bucket, where bucket depth (i.e., the maximum burst before the bucket overflows) is specified by the *burst-byte* field, and the average rate at which tokens are removed from the bucket is specified by the *rate-bps* option.

EXAMPLE

This example creates a policy called "rd-policy," uses the class command to specify the previously defined "rd-class," uses the set command to classify the service that incoming packets will receive, and then uses the **police** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 1522 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set ip dscp 3
```

```
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

set

This command services IP traffic by setting a CoS or DSCP value in a matching packet (as specified by the match command). Use the **no** form to remove the traffic classification.

SYNTAX

[**no**] **set** {**cos** *new-cos* | **ip dscp** *new-dscp*}

new-cos - New Class of Service (CoS) value. (Range: 0-7)

new-dscp - New Differentiated Service Code Point (DSCP) value. (Range: 0-63)

DEFAULT SETTING

None

COMMAND MODE

Policy Map Class Configuration

EXAMPLE

This example creates a policy called "rd-policy," uses the class command to specify the previously defined "rd-class," uses the **set** command to classify the service that incoming packets will receive, and then uses the police command to limit the average bandwidth to 100,000 Kbps, the burst rate to 1522 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

service-policy

This command applies a policy map defined by the **policy-map** command to the ingress side of a particular interface. Use the **no** form to remove this mapping.

SYNTAX

[**no**] **service-policy input** *policy-map-name*

input - Apply to the input traffic.

policy-map-name - Name of the policy map for this interface. (Range: 1-16 characters)

DEFAULT SETTING

No policy map is attached to an interface.

COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE
- Only one policy map can be assigned to an interface.
- First define a class map, then define a policy map, and finally use the **service-policy** command to bind the policy map to the required interface.
- The switch does not allow a policy map to be bound to an interface for egress traffic.

EXAMPLE
This example applies a service policy to an ingress interface.

```
Console(config)#interface ethernet 1/1
Console(config-if)#service-policy input rd-policy
Console(config-if)#
```

show class-map

This command displays the QoS class maps which define matching criteria used for classifying traffic.

SYNTAX

show class-map [*class-map-name*]

class-map-name - Name of the class map. (Range: 1-16 characters)

DEFAULT SETTING
Displays all class maps.

COMMAND MODE
Privileged Exec

EXAMPLE

```
Console#show class-map
Class Map match-any rd-class#1
Description:
 Match ip dscp 10
 Match access-list rd-access
 Match ip dscp 0

Class Map match-any rd-class#2
 Match ip precedence 5

Class Map match-any rd-class#3
 Match vlan 1

Console#
```

show policy-map

This command displays the QoS policy maps which define classification criteria for incoming traffic, and may include policers for bandwidth limitations.

SYNTAX

show policy-map [*policy-map-name* [**class** *class-map-name*]]

policy-map-name - Name of the policy map. (Range: 1-16 characters)

class-map-name - Name of the class map. (Range: 1-16 characters)

DEFAULT SETTING

Displays all policy maps and all classes.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show policy-map
Policy Map rd-policy
Description:
 class rd-class
 set phb 3
Console#show policy-map rd-policy class rd-class
Policy Map rd-policy
 class rd-class
 set phb 3
Console#
```

show policy-map interface

This command displays the service policy assigned to the specified interface.

SYNTAX

show policy-map interface *interface* **input**

interface

unit/port

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show policy-map interface 1/5 input
Service-policy rd-policy
Console#
```

40 MULTICAST FILTERING COMMANDS

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting a service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

Table 131: Multicast Filtering Commands

Command Group	Function
IGMP Snooping	Configures multicast groups via IGMP snooping or static assignment, sets the IGMP version, displays current snooping settings, and displays the multicast service and group members
IGMP Query	Configures IGMP query parameters for multicast filtering at Layer 2
Static Multicast Routing	Configures static multicast router ports which forward all inbound multicast traffic to the attached VLANs
IGMP Filtering and Throttling	Configures IGMP filtering and throttling
Multicast VLAN Registration	Configures a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, preserving security and data isolation for normal traffic

IGMP SNOOPING

This section describes commands used to configure IGMP snooping on the switch.

Table 132: IGMP Snooping Commands

Command	Function	Mode
ip igmp snooping	Enables IGMP snooping	GC
ip igmp snooping leave-proxy	Enables IGMP leave proxy on the switch	GC
ip igmp snooping priority	Assigns a priority to all multicast traffic	GC
ip igmp snooping version	Configures the IGMP version for snooping	GC
ip igmp snooping vlan static	Adds an interface as a member of a multicast group	GC
ip igmp snooping immediate-leave	Immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate-leave is enabled for the parent VLAN	IC
show ip igmp snooping	Shows the IGMP snooping, proxy, and query configuration	PE

Table 132: IGMP Snooping Commands (Continued)

Command	Function	Mode
show ip igmp snooping groups	Shows known multicast addresses learned through IGMP snooping	PE
show mac-address-table multicast	Shows the IGMP snooping multicast list	PE

ip igmp snooping

This command enables IGMP snooping globally on the switch. Use the **no** form to disable it.

SYNTAX

[**no**] **ip igmp snooping**

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

EXAMPLE

The following example enables IGMP snooping.

```
Console(config)#ip igmp snooping
Console(config)#
```

ip igmp snooping leave-proxy

This command enables IGMP leave proxy on the switch. Use the **no** form to disable the feature.

SYNTAX

[**no**] **ip igmp snooping leave-proxy**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- This function is only effective if IGMP snooping is enabled.
- The IGMP snooping leave-proxy feature suppresses all unnecessary IGMP leave messages so that the non-querier switch forwards an IGMP leave packet only when the last dynamic member port leaves a multicast group.

- The leave-proxy feature does not function when a switch is set as the querier.
- When the switch a non-querier, the receiving port is not the last dynamic member port in the group, the receiving port is not a router port, and no IGMPv1 member port exists in the group, the switch will generate and send a GS-query to the member port which received the leave message, and then start the last member query timer for that port.
- When the conditions in the preceding item all apply, except that the receiving port is a router port, then the switch will not send a GS-query, but will immediately start the last member query timer for that port.

EXAMPLE

```
Console(config)#ip igmp snooping leave-proxy
Console(config)#
```

ip igmp snooping priority

This command assigns a priority to all multicast traffic. Use the **no** form to restore the default setting.

SYNTAX

ip igmp snooping priority *priority*

no ip igmp snooping priority

priority - The CoS priority assigned to all multicast traffic. (Range: 0-6, where 6 is the highest priority)

DEFAULT SETTING

2

COMMAND MODE

Global Configuration

COMMAND USAGE

This command can be used to set a high priority for low-latency multicast traffic such as a video-conference, or to set a low priority for normal multicast traffic not sensitive to latency.

EXAMPLE

```
Console(config)#ip igmp snooping priority 6
Console(config)#
```

RELATED COMMANDS

show ip igmp snooping (870)

ip igmp snooping version

This command configures the IGMP snooping version. Use the **no** form to restore the default.

SYNTAX

ip igmp snooping version {**1** | **2** | **3**}

no ip igmp snooping version

vlan-id - VLAN ID (Range: 1-4093)

1 - IGMP Version 1

2 - IGMP Version 2

3 - IGMP Version 3

DEFAULT SETTING

Global: IGMP Version 2

COMMAND MODE

Global Configuration

COMMAND USAGE

This command configures the IGMP report/query version used by IGMP snooping. Versions 1 - 3 are all supported, and versions 2 and 3 are backward compatible, so the switch can operate with other devices, regardless of the snooping version employed.

EXAMPLE

The following configures IGMP snooping to version 1.

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

ip igmp snooping vlan static

This command adds a port to a multicast group. Use the **no** form to remove the port.

SYNTAX

[**no**] **ip igmp snooping vlan** *vlan-id* **static** *ip-address interface*

vlan-id - VLAN ID (Range: 1-4094)

ip-address - IP address for multicast group

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING
None

COMMAND MODE
Global Configuration

COMMAND USAGE
- Static multicast entries are never aged out.
- When a multicast entry is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

EXAMPLE
The following shows how to statically configure a multicast group on a port.

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet 1/5
Console(config)#
```

ip igmp snooping immediate-leave

This command immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate-leave is enabled for the parent VLAN. Use the **no** form to restore the default.

SYNTAX

[**no**] **ip igmp snooping immediate-leave**

DEFAULT SETTING
Disabled

COMMAND MODE
Interface Configuration (VLAN)

COMMAND USAGE
- If immediate-leave is *not* used, a multicast router (or querier) will send a group-specific query message when an IGMPv2/v3 group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the time-out period specified by the ip igmp snooping query-max-response-time command.
- If immediate-leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one IGMP-enabled device, either a service host or a neighbor running IGMP snooping.
- This command is only effective if IGMP snooping is enabled, and IGMPv2 or IGMPv3 snooping is used.

EXAMPLE

The following shows how to enable immediate leave.

```
Console(config)#ip igmp snooping immediate-leave
Console(config)#
```

show ip igmp snooping

This command shows the IGMP snooping, proxy, and query configuration settings.

COMMAND MODE

Privileged Exec

COMMAND USAGE

This command displays global and VLAN-specific IGMP configuration settings. See "Configuring IGMP Snooping and Query Parameters" for a description of the displayed items.

EXAMPLE

The following shows the current IGMP snooping configuration:

```
Console#show ip igmp snooping
 Service Status:           Enabled
 Querier Status:           Disabled
 Leave proxy status:       Disabled
 Priority:                 2
 Query Count:              2
 Query Interval:           125 sec
 Query Max Response Time: 10 sec
 Router Port Expire Time: 300 sec
 Immediate Leave Processing: Disabled on all VLANs
 IGMP Snooping Version:    Version 2
 ------------------------------------
 VLAN 1:
 --------
 IGMP snooping: Enabled

 VLAN 4093:
 --------
 IGMP snooping: Enabled

Console#
```

show ip igmp snooping groups

This command shows known multicast addresses learned through IGMP snooping.

SYNTAX

show ip igmp snooping groups

COMMAND MODE

Privileged Exec

EXAMPLE

The following shows the multicast entries learned through IGMP snooping:

```
Console#show ip igmp snooping groups
 VLAN IP Addressses   Member Port  Type
 ---- --------------- ------------ -------------
    1 239.255.255.250     Eth 1/ 1 IGMP Snooping
Console#
```

show mac-address-table multicast

This command shows known multicast addresses.

SYNTAX

show mac-address-table multicast [**vlan** *vlan-id*] [**user** | **igmp-snooping**]

vlan-id - VLAN ID (1-4094)

user - Display only the user-configured multicast entries.

igmp-snooping - Display only entries learned through IGMP snooping.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

Member types displayed include IGMP or USER, depending on selected options.

EXAMPLE

The following shows the multicast entries learned through IGMP snooping for VLAN 1:

```
Console#show mac-address-table multicast vlan 1 igmp-snooping
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1       224.1.2.3      Eth1/11    IGMP
Console#
```

IGMP QUERY COMMANDS

This section describes commands used to configure IGMP query on the switch.

Table 133: IGMP Query Commands

Command	Function	Mode
ip igmp snooping querier	Allows this device to act as the querier for IGMP snooping	GC
ip igmp snooping query-count	Configures the query count	GC
ip igmp snooping query-interval	Configures the query interval	GC
ip igmp snooping query-max-response-time	Configures the report delay	GC
ip igmp snooping router-port-expire-time	Configures the query timeout	GC

ip igmp snooping querier

This command enables the switch as an IGMP querier. Use the **no** form to disable it.

SYNTAX

[**no**] **ip igmp snooping querier**

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- IGMP snooping querier is not supported for IGMPv3 snooping.
- If enabled, the switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.

EXAMPLE

```
Console(config)#ip igmp snooping querier
Console(config)#
```

RELATED COMMANDS

ip igmp snooping version (868)

ip igmp snooping query-count

This command configures the query count. Use the **no** form to restore the default count.

SYNTAX

ip igmp snooping query-count *count*

no ip igmp snooping query-count

count - The maximum number of queries issued for which there has been no response before the switch takes action to drop a client from the multicast group. (Range: 2-10)

DEFAULT SETTING

2 times

COMMAND MODE

Global Configuration

COMMAND USAGE

The query count defines how long the querier waits for a response from a multicast client before taking action. If a querier has sent a number of queries defined by this command, but a client has not responded, a countdown timer is started using the time defined by **ip igmp snooping query-max- response-time**. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

EXAMPLE

The following shows how to configure the query count to 10:

```
Console(config)#ip igmp snooping query-count 10
Console(config)#
```

RELATED COMMANDS

ip igmp snooping query-max-response-time (874)

ip igmp snooping query-interval

This command configures the query interval. Use the **no** form to restore the default.

SYNTAX

ip igmp snooping query-interval *seconds*

no ip igmp snooping query-interval

seconds - The frequency at which the switch sends IGMP host-query messages. (Range: 60-125)

DEFAULT SETTING

125 seconds

COMMAND MODE
Global Configuration

EXAMPLE
The following shows how to configure the query interval to 100 seconds:

```
Console(config)#ip igmp snooping query-interval 100
Console(config)#
```

ip igmp snooping query-max-response-time

This command configures the query report delay. Use the **no** form to restore the default.

SYNTAX

ip igmp snooping query-max-response-time *seconds*

no ip igmp snooping query-max-response-time

seconds - The report delay advertised in IGMP queries. (Range: 5-25)

DEFAULT SETTING
10 seconds

COMMAND MODE
Global Configuration

COMMAND USAGE
- The switch must be using IGMPv2/v3 for this command to take effect.
- This command defines the time after a query, during which a response is expected from a multicast client. If a querier has sent a number of queries defined by the ip igmp snooping query-count command, but a client has not responded, a countdown timer is started using an initial value set by this command. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

EXAMPLE
The following shows how to configure the maximum response time to 20 seconds:

```
Console(config)#ip igmp snooping query-max-response-time 20
Console(config)#
```

RELATED COMMANDS
ip igmp snooping version (868)

ip igmp snooping router-port-expire-time

This command configures the querier timeout. Use the **no** form to restore the default.

SYNTAX

ip igmp snooping router-port-expire-time *seconds*

no ip igmp snooping router-port-expire-time

seconds - The time the switch waits after the previous querier stops before it considers it to have expired. (Range: 1-65535; Recommended Range: 300-500)

DEFAULT SETTING

300 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

The switch must use IGMPv2/v3 snooping for this command to take effect.

EXAMPLE

The following shows how to configure the time out to 400 seconds:

```
Console(config)#ip igmp snooping router-port-expire-time 400
Console(config)#
```

RELATED COMMANDS

ip igmp snooping version (868)

STATIC MULTICAST ROUTING

This section describes commands used to configure static multicast routing on the switch.

Table 134: Static Multicast Interface Commands

Command	Function	Mode
ip igmp snooping vlan mrouter	Adds a multicast router port	GC
show ip igmp snooping mrouter	Shows multicast router ports	PE

ip igmp snooping vlan mrouter

This command statically configures a (Layer 2) multicast router port on the specified VLAN. Use the **no** form to remove the configuration.

SYNTAX

[**no**] **ip igmp snooping vlan** *vlan-id* **mrouter** *interface*

vlan-id - VLAN ID (Range: 1-4094)

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

No static multicast router ports are configured.

COMMAND MODE

Global Configuration

COMMAND USAGE

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router or switch connected over the network to an interface (port or trunk) on this switch, that interface can be manually configured to join all the current multicast groups.

EXAMPLE

The following shows how to configure port 10 as a multicast router port within VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/10
Console(config)#
```

show ip igmp snooping mrouter

This command displays information on statically configured and dynamically learned multicast router ports.

SYNTAX

show ip igmp snooping mrouter [**vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

DEFAULT SETTING

Displays multicast router ports for all configured VLANs.

COMMAND MODE

Privileged Exec

COMMAND USAGE

Multicast router port types displayed include Static.

EXAMPLE

The following shows the ports in VLAN 1 which are attached to multicast routers.

```
Console#show ip igmp snooping mrouter vlan 1
 VLAN M'cast Router Ports Type
 ---- ------------------- --------
    1            Eth 1/10  Static
Console#
```

IGMP FILTERING AND THROTTLING

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The IGMP filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and IGMP throttling limits the number of simultaneous multicast groups a port can join.

Table 135: IGMP Filtering and Throttling Commands

Command	Function	Mode
ip igmp filter	Enables IGMP filtering and throttling on the switch	GC
ip igmp profile	Sets a profile number and enters IGMP filter profile configuration mode	GC
permit, deny	Sets a profile access mode to permit or deny	IPC
range	Specifies one or a range of multicast addresses for a profile	IPC
ip igmp filter	Assigns an IGMP filter profile to an interface	IC
ip igmp max-groups	Specifies an IGMP throttling number for an interface	IC
ip igmp max-groups action	Sets the IGMP throttling action for an interface	IC
show ip igmp filter	Displays the IGMP filtering status	PE
show ip igmp profile	Displays IGMP profiles and settings	PE
show ip igmp throttle interface	Displays the IGMP throttling setting for interfaces	PE

ip igmp filter (Global Configuration)

This command globally enables IGMP filtering and throttling on the switch. Use the **no** form to disable the feature.

SYNTAX

[**no**] **ip igmp filter**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- IGMP filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. An IGMP filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, IGMP join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the IGMP join report is forwarded as normal. If a requested multicast group is denied, the IGMP join report is dropped.
- IGMP filtering and throttling only applies to dynamically learned multicast groups, it does not apply to statically configured groups.
- The IGMP filtering feature operates in the same manner when MVR is used to forward multicast traffic.

EXAMPLE

```
Console(config)#ip igmp filter
Console(config)#
```

ip igmp profile

This command creates an IGMP filter profile number and enters IGMP profile configuration mode. Use the **no** form to delete a profile number.

SYNTAX

[**no**] **ip igmp profile** *profile-number*

profile-number - An IGMP filter profile number. (Range: 1-4294967295)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

A profile defines the multicast groups that a subscriber is permitted or denied to join. The same profile can be applied to many interfaces, but only one profile can be assigned to one interface. Each profile has only one access mode; either permit or deny.

EXAMPLE

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#
```

permit, deny

This command sets the access mode for an IGMP filter profile. Use the **no** form to delete a profile number.

SYNTAX

{**permit** | **deny**}

DEFAULT SETTING

Deny

COMMAND MODE

IGMP Profile Configuration

COMMAND USAGE

- Each profile has only one access mode; either permit or deny.
- When the access mode is set to permit, IGMP join reports are processed when a multicast group falls within the controlled range. When the access mode is set to deny, IGMP join reports are only processed when a multicast group is not in the controlled range.

EXAMPLE

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#permit
Console(config-igmp-profile)#
```

range

This command specifies multicast group addresses for a profile. Use the **no** form to delete addresses from a profile.

SYNTAX

[**no**] **range** *low-ip-address* [*high-ip-address*]

low-ip-address - A valid IP address of a multicast group or start of a group range.

high-ip-address - A valid IP address for the end of a multicast group range.

DEFAULT SETTING
None

COMMAND MODE
IGMP Profile Configuration

COMMAND USAGE
Enter this command multiple times to specify more than one multicast address or address range for a profile.

EXAMPLE

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#range 239.1.1.1
Console(config-igmp-profile)#range 239.2.3.1 239.2.3.100
Console(config-igmp-profile)#
```

ip igmp filter (Interface Configuration)

This command assigns an IGMP filtering profile to an interface on the switch. Use the **no** form to remove a profile from an interface.

SYNTAX

[**no**] **ip igmp filter** *profile-number*

profile-number - An IGMP filter profile number. (Range: 1-4294967295)

DEFAULT SETTING
None

COMMAND MODE
Interface Configuration

COMMAND USAGE
- The IGMP filtering profile must first be created with the ip igmp profile command before it can be assigned to an interface.
- Only one profile can be assigned to an interface.
- A profile can also be assigned to a trunk interface. When ports are configured as trunk members, the trunk uses the filtering profile assigned to the first port member in the trunk.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp filter 19
Console(config-if)#
```

ip igmp max-groups

This command sets the IGMP throttling number for an interface on the switch. Use the **no** form to restore the default setting.

SYNTAX

ip igmp max-groups *number*

no ip igmp max-groups

number - The maximum number of multicast groups an interface can join at the same time. (Range: 0-256)

DEFAULT SETTING

256

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either "deny" or "replace" as specified by the ip igmp max-groups action command. If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

- IGMP throttling can also be set on a trunk interface. When ports are configured as trunk members, the trunk uses the throttling settings of the first port member in the trunk.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups 10
Console(config-if)#
```

ip igmp max-groups action

This command sets the IGMP throttling action for an interface on the switch.

SYNTAX

ip igmp max-groups action {**replace** | **deny**}

replace - The new multicast group replaces an existing group.

deny - The new multicast group join report is dropped.

DEFAULT SETTING

Deny

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

When the maximum number of groups is reached on a port, the switch can take one of two actions; either "deny" or "replace." If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups action replace
Console(config-if)#
```

show ip igmp filter

This command displays the global and interface settings for IGMP filtering.

SYNTAX

show ip igmp filter [**interface** *interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip igmp filter
IGMP filter enabled
Console#show ip igmp filter interface ethernet 1/1
Ethernet 1/1 information
--------------------------------
 IGMP Profile 19
  deny
  range 239.1.1.1 239.1.1.1
  range 239.2.3.1 239.2.3.100
Console#
```

show ip igmp profile

This command displays IGMP filtering profiles created on the switch.

SYNTAX

show ip igmp profile [*profile-number*]

profile-number - An existing IGMP filter profile number. (Range: 1-4294967295)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip igmp profile
IGMP Profile 19
IGMP Profile 50
Console#show ip igmp profile 19
IGMP Profile 19
  deny
  range 239.1.1.1 239.1.1.1
  range 239.2.3.1 239.2.3.100
Console#
```

show ip igmp throttle interface

This command displays the interface settings for IGMP throttling.

SYNTAX

show ip igmp throttle interface [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

Using this command without specifying an interface displays all interfaces.

EXAMPLE

```
Console#show ip igmp throttle interface ethernet 1/1
Eth  1/1 Information
  status : true
  action : deny
  max multicast groups : 32
  current multicast groups : 0

Console#
```

MULTICAST VLAN REGISTRATION

This section describes commands used to configure Multicast VLAN Registration (MVR). A single network-wide VLAN can be used to transmit multicast traffic (such as television channels) across a service provider's network. Any multicast traffic entering an MVR VLAN is sent to all subscribers. This can significantly reduce to processing overhead required to dynamically monitor and establish the distribution tree for a normal multicast VLAN. Also note that MVR maintains the user isolation and data security provided by VLAN segregation by passing only multicast traffic into other VLANs to which the subscribers belong.

Table 136: Multicast VLAN Registration Commands

Command	Function	Mode
mvr	Globally enables MVR	GC
mvr group	Statically configures MVR group address(es)	GC
mvr priority	Assigns a priority to all multicast traffic in the MVR VLAN	GC
mvr receiver-group	Specifies groups to be managed through the MVR receiver VLAN	GC
mvr receiver-vlan	Allows multicast traffic to be forwarded from the specified receiver VLAN without revealing the identity of the MVR VLAN in tagged frames	GC
mvr unspecified-source-ip	Sets the source IP address to an unspecified address in IGMP report and leave messages forwarded to the MVR VLAN	GC
mvr vlan	Specifies the MVR VLAN identifier	GC
mvr group	Statically binds a multicast group to a port	IC
mvr immediate	Enables immediate leave capability	IC
mvr static-receiver-group	Statically assigns a multicast receiver group to an interface	
mvr type	Configures an interface as an MVR receiver or source port	IC
show mvr	Shows information about the global MVR configuration settings, interfaces attached to the MVR VLAN, or the multicast groups assigned to the MVR VLAN	PE

mvr

This command enables Multicast VLAN Registration (MVR) globally on the switch. Use the **no** form of this command to globally disable MVR.

SYNTAX

[**no**] **mvr**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- IGMP snooping must be enabled to a allow a subscriber to dynamically join or leave an MVR group (see the ip igmp snooping command). Note that only IGMP version 2 or 3 hosts can issue multicast join or leave messages.

EXAMPLE

The following example enables MVR globally.

```
Console(config)#mvr
Console(config)#
```

mvr group

This command statically configures MVR multicast group IP address(es). Use the **no** form of this command to remove a specific address or range of addresses.

SYNTAX

[**no**] **mvr group** *ip-address* [*count*]

group - Defines a multicast service sent to all attached subscribers.

ip-address - IP address for an MVR multicast group.
(Range: 224.0.1.0 - 239.255.255.255)

count - The number of contiguous MVR group addresses.
(Range: 1-255)

DEFAULT SETTING

No MVR group address is defined.

COMMAND MODE

Global Configuration

COMMAND USAGE

- Use this command to statically configure all multicast group addresses that will join the MVR VLAN. Any multicast data associated an MVR group is sent from all source ports, and to all receiver ports that have registered to receive data from that multicast group.

- The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.
- IGMP snooping and MVR can share a maximum number of 255 groups. Any multicast streams received in excess of this limitation will be flooded to all ports in the associated VLAN.

EXAMPLE

The following example configures a range of MVR group addresses:

```
Console(config)#mvr group 228.1.23.1 10
Console(config)#
```

mvr priority

This command assigns a priority to all multicast traffic in the MVR VLAN. Use the **no** form of this command to restore the default setting.

SYNTAX

mvr priority *priority*

no mvr priority

priority - The CoS priority assigned to all multicast traffic forwarded into the MVR VLAN. (Range: 0-6, where 6 is the highest priority)

DEFAULT SETTING

2

COMMAND MODE

Global Configuration

COMMAND USAGE

This command can be used to set a high priority for low-latency multicast traffic such as a video-conference, or to set a low priority for normal multicast traffic not sensitive to latency.

EXAMPLE

```
Console(config)#mvr priority 6
Console(config)#
```

RELATED COMMANDS

show mvr (893)

mvr receiver-group

This command specifies MVR multicast groups to be managed through the MVR receiver VLAN. Use the **no** form of this command to remove a group from the receiver VLAN.

SYNTAX

[**no**] **mvr receiver-group** *ip-address*

ip-address - IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- Multicast traffic forwarded to subscribers is normally stripped of frame tags to prevent the hosts from discovering the identity of the MVR VLAN. To allow multicast traffic with tagged frames to be sent to subscribers without revealing the identity of the MVR VLAN, both the **mvr receiver-group** and mvr receiver-vlan must be specifically defined. If a port is manually assigned to the receiver VLAN as a tagged member, multicast traffic forwarded to the subscriber will also carry tags.
- The **mvr receiver-group** and mvr group cannot be configured with the same addresses.

EXAMPLE

```
Console(config)#mvr receiver group 228.1.24.1
Console(config)#
```

RELATED COMMANDS

mvr receiver-vlan (887)

mvr receiver-vlan

This command allows multicast traffic to be forwarded from the specified receiver VLAN without revealing the identity of the MVR VLAN in tagged frames. Use the **no** form of this command to remove the receiver VLAN.

SYNTAX

mvr receiver-vlan *vlan-id*

no mvr receiver-vlan

vlan-id - MVR receiver VLAN ID (Range: 1-4094)

DEFAULT SETTING

None

COMMAND MODE
Global Configuration

COMMAND USAGE
- Multicast traffic forwarded to subscribers is normally stripped of frame tags to prevent the hosts from discovering the identity of the MVR VLAN. To allow multicast traffic with tagged frames to be sent to subscribers without revealing the identity of the MVR VLAN, both the mvr receiver-group and **mvr receiver-vlan** must be specifically defined. If a port is manually assigned to the receiver VLAN as a tagged member, multicast traffic forwarded to the subscriber will also carry tags.

- The **mvr receiver-vlan** cannot be configured with the same VLAN used by other types of VLANs (such as 802.1Q or private VLANs).

EXAMPLE
```
Console(config)#mvr receiver-vlan 228
Console(config)#
```

RELATED COMMANDS
mvr receiver-group (887)

mvr unspecified-source-ip

This command sets the source IP address to an unspecified address in IGMP report and leave messages forwarded to the MVR VLAN. Use the **no** form disable this feature.

SYNTAX
[**no**] **mvr unspecified-source-ip**

DEFAULT SETTING
Disabled

COMMAND MODE
Global Configuration

COMMAND USAGE
- When this feature is enabled, the source IP address is set to an unspecified address in IGMP report and leave messages forwarded to the MVR VLAN. In this way the source of all multicast streams can be hidden from downstream hosts within the MVR VLAN.

- However, note that when this feature is enabled, the source IP address will not be changed in IGMP report, leave and query control packets sent from the MVR VLAN on this switch to upstream multicast routers.

EXAMPLE

```
Console(config)#mvr unspecified-source-ip
Console(config)#
```

mvr vlan

This command specifies the MVR VLAN identifier. Use the **no** form of this command to restore the default MVR VLAN.

SYNTAX

mvr vlan *vlan-id*

no mvr vlan

vlan-id - MVR VLAN ID (Range: 1-4094)

DEFAULT SETTING

MVR VLAN ID is 1.

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command specifies the VLAN through which MVR multicast data is received. This is the VLAN to which all source ports must be assigned.
- The VLA N specified by this command must be an existing VLAN configured with the vlan command.
- MVR source ports can be configured as members of the MVR VLAN using the switchport allowed vlan command and switchport native vlan command, but MVR receiver ports should not be statically configured as members of this VLAN.

EXAMPLE

```
Console(config)#mvr vlan 228
Console(config)#
```

mvr group

This command statically binds a multicast group to a port which will receive long-term multicast streams associated with a stable set of hosts. Use the **no** form to restore the default settings.

SYNTAX

[**no**] **mvr group** *ip-address*

ip-address - Statically configures an interface to receive multicast traffic from the IP address specified for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

DEFAULT SETTING
No receiver port is a member of any configured multicast group.

COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE
- Multicast groups can be statically assigned to a receiver port using this command.
- The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.

EXAMPLE
The following statically assigns a multicast group to a receiver port:

```
Console(config)#interface ethernet 1/7
Console(config-if)#mvr type receiver
Console(config-if)#mvr vlan 3 group 225.0.0.5
Console(config-if)#
```

mvr immediate

This command causes the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group. Use the **no** form to restore the default settings.

SYNTAX
[**no**] **mvr immediate**

DEFAULT SETTING
Disabled

COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE
- This option only applies to an interface configured as an MVR receiver using the mvr type command).
- Immediate leave applies only to receiver ports. When enabled, the receiver port is immediately removed from the multicast group identified in the leave message. When immediate leave is disabled, the switch follows the standard rules by sending a group-specific query to the receiver port and waiting for a response to determine if there are any remaining subscribers for that multicast group before removing the port from the group list.
- Using immediate leave can speed up leave latency, but should only be enabled on a port attached to one multicast subscriber to avoid

disrupting services to other group members attached to the same interface.

- Immediate leave does not apply to multicast groups which have been statically assigned to a port.

EXAMPLE

The following enables immediate leave on a receiver port.

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr immediate
Console(config-if)#
```

mvr static-receiver-group

This command statically assigns a multicast receiver group to an interface.

SYNTAX

[**no**] **mvr static-receiver-group** *ip-address*

ip-address - Statically configures an interface to receive multicast traffic from the IP address specified for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

DEFAULT SETTING

No receiver port is a member of any configured multicast group.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

The specified multicast service must already be configured as a receiver group which will be managed through the MVR receiver VLAN (see the mvr receiver-group and mvr receiver-vlan commands).

EXAMPLE

The following configures a static receiver group on port 5.

```
Console(config)#mvr
Console(config)#mvr receiver-group 228.1.24.1
Console(config)#mvr receiver-vlan 2
Console(config)#interface ethernet 1/5
Console(config-if)#mvr static-receiver-group 228.1.24.1
Console(config-if)#
```

mvr type

This command configures an interface as an MVR receiver or source port. Use the **no** form to restore the default settings.

SYNTAX

[**no**] **mvr type** {**receiver** | **source**}

receiver - Configures the interface as a subscriber port that can receive multicast data.

source - Configures the interface as an uplink port that can send and receive multicast data for the configured multicast groups.

DEFAULT SETTING

The port type is not defined.

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- A port which is not configured as an MVR receiver or source port can use IGMP snooping to join or leave multicast groups using the standard rules for multicast filtering.
- Receiver ports can belong to different VLANs, but should not be configured as a member of the MVR VLAN. If statically configured as a member of the MVR VLAN using the switchport allowed vlan command, the receiver port's MVR status will be inactive.

  IGMP snooping can be used to allow a receiver port to dynamically join or leave multicast groups sourced through the MVR VLAN. Multicast groups can also be statically assigned to a receiver port using the mvr group (Interface Configuration) command.

  Also, note that VLAN membership for MVR receiver ports cannot be set to trunk mode (see the switchport mode command).
- One or more interfaces may be configured as MVR source ports. A source port is able to both receive and send data for multicast groups which it has joined through IGMP snooping or which have been assigned through the mvr group (Global Configuration) command.
- IGMP snooping must be enabled to a allow a subscriber to dynamically join or leave an MVR group (see the ip igmp snooping command). Note that only IGMP version 2 or 3 hosts can issue multicast join or leave messages.

EXAMPLE

The following configures one source port and several receiver ports on the switch.

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr type source
Console(config-if)#exit
Console(config)#interface ethernet 1/6
```

```
Console(config-if)#mvr type receiver
Console(config-if)#exit
Console(config)#interface ethernet 1/7
Console(config-if)#mvr type receiver
Console(config-if)#
```

show mvr

This command shows information about the global MVR configuration settings when entered without any keywords, the interfaces attached to the MVR VLAN using the **interface** keyword, the multicast groups assigned to the MVR VLAN using the **members** keyword or the interfaces assigned to MVR receiver groups using the **receiver-group members** keyword.

SYNTAX

show mvr [**interface** [*interface*] | **members** [*ip-address*]] | **receiver-group members** [*ip-address*]]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

ip-address - IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

DEFAULT SETTING

Displays global configuration settings for MVR when no keywords are used.

COMMAND MODE

Privileged Exec

EXAMPLE

The following shows the global MVR settings:

```
Console#show mvr
MVR Status:                              Enabled
MVR Running Status:                      True
MVR Multicast VLAN:                      1
MVR priority:                            2
MVR Max Multicast Groups:                1024
MVR Current Multicast Groups:            12
MVR Unspecified Source IP:               Disabled
MVR Receiver VLAN:                        2
MVR Supported Receiver Multicast Groups: 5
MVR Used Receiver Multicast Groups:       2

Console#
```

Table 137: show mvr - display description

Field	Description
MVR Status	Shows if MVR is globally enabled on the switch.
MVR Running Status	Indicates whether or not all necessary conditions in the MVR environment are satisfied. (Running status is true as long as MVR Status is enabled, and the specified MVR VLAN exists.)
MVR Multicast VLAN	Shows the VLAN used to transport all MVR multicast traffic.
MVR Priority	The priority assigned to all multicast traffic in the MVR VLAN.
MVR Max Multicast Groups	Shows the maximum number of multicast groups which can assigned to the MVR VLAN.
MVR Current Multicast Groups	Shows the number of multicast groups currently assigned to the MVR VLAN.
MVR Unspecified Source IP	Shows if an unspecified source address is used in IGMP report and leave messages forwarded to the MVR VLAN.
MVR Receiver VLAN	VLAN used to froward multicast traffic with tagged frames without revealing the identity of the MVR VLAN
MVR Supported Receiver Multicast Groups	Number of multicast groups to be managed through the receiver VLAN
MVR Used Receiver Multicast Groups	Number of multicast groups currently active within the receiver VLAN

The following displays information about the interfaces attached to the MVR VLAN:

```
Console#show mvr interface
Port    Type            Status          Immediate Leave
------- --------        -------------   ---------------
eth1/1  SOURCE          ACTIVE/UP         Disabled
eth1/2  RECEIVER        ACTIVE/UP         Disabled
eth1/5  RECEIVER        INACTIVE/DOWN     Disabled
eth1/6  RECEIVER        INACTIVE/DOWN     Disabled
eth1/7  RECEIVER        INACTIVE/DOWN     Disabled
Console#
```

Table 138: show mvr interface - display description

Field	Description
Port	Shows interfaces attached to the MVR.
Type	Shows the MVR port type.
Status	Shows the MVR status and interface status. MVR status for source ports is "ACTIVE" if MVR is globally enabled on the switch. MVR status for receiver ports is "ACTIVE" only if there are subscribers receiving multicast traffic from one of the MVR groups, or a multicast group has been statically assigned to an interface.
Immediate Leave	Shows if immediate leave is enabled or disabled.

The following shows information about the interfaces associated with multicast groups assigned to the MVR VLAN:

```
Console#show mvr members
MVR Group IP      Status    Receiver VLAN  Members
----------------  --------  -------------  -------
225.0.0.1         ACTIVE    VLAN2          eth1/1(d), eth1/2(s)
225.0.0.2         INACTIVE  None           None
225.0.0.3         INACTIVE  None           None
225.0.0.4         INACTIVE  None           None
225.0.0.5         INACTIVE  None           None
225.0.0.6         INACTIVE  None           None
225.0.0.7         INACTIVE  None           None
225.0.0.8         INACTIVE  None           None
225.0.0.9         INACTIVE  None           None
225.0.0.10        INACTIVE  None           None
Console#
```

Table 139: show mvr members - display description

Field	Description
MVR Group IP	Multicast groups assigned to the MVR VLAN.
Status	Shows whether or not the there are active subscribers for this multicast group. Note that this field will also display "INACTIVE" if MVR is globally disabled.
Receiver VLAN	VLAN used to froward multicast traffic with tagged frames without revealing the identity of the MVR VLAN
Members	Shows the interfaces with subscribers for multicast services provided through the MVR VLAN. Also shows if an interface has dynamically joined a multicast group (**d**), or if a multicast group has been statically bound to the interface (**s**).

The following shows the interfaces which have joined MVR receiver groups, and the status of MVR traffic for each group:

```
Console#show mvr receiver-group members
MVR Group IP      Status    Members
----------------  --------  -------
224.0.0.1         ACTIVE    eth1/1
224.0.0.2         INACTIVE  None
224.0.1.1         INACTIVE  None
224.0.1.2         INACTIVE  None
224.0.1.3         INACTIVE  None
Console#
```

Table 140: show mvr receiver members - display description

Field	Description
MVR Group IP	Multicast groups assigned to the MVR Receiver VLAN.
Status	Shows whether or not the there are active subscribers for this multicast group. Note that this field will also display "ACTIVE" if an interface has been statically assigned to a group.
Members	Shows the interfaces with subscribers for multicast services provided through the MVR Receiver VLAN. Also shows if an interface has dynamically joined a multicast group (**d**), or if a multicast group has been statically bound to the interface (**s**).

41 MLD SNOOPING COMMANDS

Multicast Listener Discovery (MLD) snooping operates on IPv6 traffic and performs a similar function to IGMP snooping for IPv4. That is, MLD snooping dynamically configures switch ports to limit IPv6 multicast traffic so that it is forwarded only to ports with users that want to receive it. This reduces the flooding of IPv6 multicast packets in the specified VLANs.

There are two versions of the MLD protocol, version 1 and version 2. MLDv1 control packets include Listener Query, Listener Report, and Listener Done messages (equivalent to IGMPv2 query, report, and leave messages). MLDv2 control packets include MLDv2 query and report messages, as well as MLDv1 report and done messages. The switch does not support the MLD querier function, which sends out query messages to discover hosts that want to receive specific multicast services.

Remember that IGMP Snooping and MLD Snooping are independent functions, and can therefore both function at the same time.

Table 141: MLD Snooping Commands

Command	Function	Mode
ipv6 mld snooping	Enables MLD Snooping globally	GC
ipv6 mld snooping robustness	Configures the robustness variable	GC
ipv6 mld snooping router-port-expire-time	Configures the router port expire time	GC
ipv6 mld snooping unknown-multicast mode	Sets an action for unknown multicast packets	GC
ipv6 mld snooping version	Configures the MLD Snooping version	GC
ipv6 mld snooping vlan mrouter	Adds an IPv6 multicast router port	GC
ipv6 mld snooping vlan static	Adds an interface as a member of a multicast group	GC
ipv6 mld snooping immediate-leave	Removes a member port of an IPv6 multicast service if a leave packet is received at that port and MLD immediate-leave is enabled for the parent VLAN	IC
show ipv6 mld snooping	Displays MLD Snooping configuration	PE
show ipv6 mld snooping group	Displays the learned groups	PE
show ipv6 mld snooping mrouter	Displays the information of multicast router ports	PE

ipv6 mld snooping

This command enables MLD Snooping globally on the switch. Use the **no** form to disable MLD Snooping.

SYNTAX

[**no**] **ipv6 mld snooping**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

EXAMPLE

The following example enables MLD Snooping:

```
Console(config)#ipv6 mld snooping
Console(config)#
```

ipv6 mld snooping robustness

This command configures the MLD Snooping robustness variable. Use the **no** form to restore the default value.

SYNTAX

ipv6 mld snooping robustness *value*

no ipv6 mld snooping robustness

value - The number of the robustness variable. (Range: 2-10)

DEFAULT SETTING

2

COMMAND MODE

Global Configuration

COMMAND USAGE

A port will be removed from receiving a multicast service when no MLD reports are detected in response to a number of MLD queries. The robustness variable sets the number of queries on ports for which there is no report.

EXAMPLE

```
Console(config)#ipv6 mld snooping robustness 2
Console(config)#
```

ipv6 mld snooping router-port-expire-time

This command configures the MLD query timeout. Use the **no** form to restore the default.

SYNTAX

ipv6 mld snooping router-port-expire-time *time*

no ipv6 mld snooping router-port-expire-time

time - Specifies the timeout of a dynamically learned router port. (Range: 300-500 seconds)

DEFAULT SETTING

300 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

The router port expire time is the time the switch waits after the previous querier stops before it considers the router port (i.e., the interface that had been receiving query packets) to have expired.

EXAMPLE

```
Console(config)#ipv6 mld snooping router-port-expire-time 300
Console(config)#
```

ipv6 mld snooping unknown-multicast mode

This command sets the action for dealing with unknown multicast packets. Use the **no** form to restore the default.

SYNTAX

ipv6 mld snooping unknown-multicast mode {**flood** | **to-router-port**}

[**no**] **ipv6 mld snooping unknown-multicast mode**

flood - Floods the unknown multicast data packets to all ports.

to-router-port - Forwards the unknown multicast data packets to router ports.

DEFAULT SETTING

to-router-port

COMMAND MODE

Global Configuration

COMMAND USAGE

- When set to "flood," any received IPv6 multicast packets that have not been requested by a host are flooded to all ports in the VLAN.

- When set to "router-port," any received IPv6 multi cst packets that have not been requested by a host are forwarded to ports that are connected to a detected multicast router.

EXAMPLE

```
Console(config)#ipv6 mld snooping unknown-multicast mode flood
Console(config)#
```

ipv6 mld snooping version

This command configures the MLD snooping version. Use the **no** form to restore the default.

SYNTAX

ipv6 mld snooping version {**1** | **2**}

1 - MLD version 1.

2 - MLD version 2.

DEFAULT SETTING

Version 2

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#ipv6 mld snooping version 1
Console(config)#
```

ipv6 mld snooping vlan mrouter

This command statically configures an IPv6 multicast router port. Use the **no** form to remove the configuration.

SYNTAX

[**no**] **ipv6 mld snooping vlan** *vlan-id* **mrouter** *interface*

vlan-id - VLAN ID (Range: 1-4094)

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

No static multicast router ports are configured.

COMMAND MODE
Global Configuration

COMMAND USAGE
Depending on your network connections, MLD snooping may not always be able to locate the MLD querier. Therefore, if the MLD querier is a known multicast router/switch connected over the network to an interface (port or trunk) on the switch, you can manually configure that interface to join all the current multicast groups.

EXAMPLE
The following shows how to configure port 1 as a multicast router port within VLAN 1:

```
Console(config)#ipv6 mld snooping vlan 1 mrouter ethernet 1/1
Console(config)#
```

ipv6 mld snooping vlan static

This command adds a port to an IPv6 multicast group. Use the **no** form to remove the port.

SYNTAX

[**no**] **ipv6 mld snooping vlan** *vlan-id* **static** *ipv6-address interface*

vlan - VLAN ID (Range: 1-4094)

ipv6-address - An IPv6 address of a multicast group. (Format: X:X:X:X::X)

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING
None

COMMAND MODE
Global Configuration

EXAMPLE

```
Console(config)#ipv6 mld snooping vlan 1 static FF00:0:0:0:0:0:0:10C ethernet
  1/6
Console(config)#
```

ipv6 mld snooping immediate-leave

This command immediately deletes a member port of an IPv6 multicast service when a leave packet is received at that port and immediate-leave is enabled for the parent VLAN. Use the **no** form to restore the default.

SYNTAX

[**no**] **ipv6 mld snooping immediate-leave**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- If MLD immediate-leave is *not* used, a multicast router (or querier) will send a group-specific query message when an MLD group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period.
- If MLD immediate-leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one MLD-enabled device, either a service host or a neighbor running MLD snooping.

EXAMPLE

The following shows how to enable MLD immediate leave.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 mld snooping immediate-leave
Console(config-if)#
```

show ipv6 mld snooping

This command shows the current MLD Snooping configuration.

SYNTAX

show ipv6 mld snooping

COMMAND MODE

Privileged Exec

EXAMPLE

The following shows MLD Snooping configuration information

```
Console#show ipv6 mld snooping
 Service Status              : Disabled
 Robustness                  : 2
 Router Port Expiry Time     : 300 sec
 Immediate Leave             : Disabled on all VLAN
```

```
 Unknown Flood Behavior      : To Router Port
 MLD Snooping Version        : Version 2
Console#
```

show ipv6 mld snooping group

This command shows statistics about MLD Snooping groups.

SYNTAX

show ipv6 mld snooping group

COMMAND MODE

Privileged Exec

EXAMPLE

The following shows MLD Snooping group configuration information:

```
Console#show ipv6 mld snooping group

VLAN Multicast IPv6 Address                  Member port Type
---- --------------------------------------- ----------- ---------------
   1                               FF08::10C Eth 1/ 6    User
Console#
```

show ipv6 mld snooping mrouter

This command shows MLD Snooping multicast router information.

SYNTAX

show ipv6 mld snooping mrouter <**vlan** *vlan-id*>

vlan-id - A VLAN identification number. (Range: 1-4094)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ipv6 mld snooping mrouter vlan 1
 VLAN Multicast Router Port Type
 ---- -------------------- ---------
    1 Eth 1/ 2             Static

Console#
```

42 LLDP COMMANDS

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power, inventory, and device location details. LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

Table 142: LLDP Commands

Command	Function	Mode
lldp	Enables LLDP globally on the switch	GC
lldp holdtime-multiplier	Configures the time-to-live (TTL) value sent in LLDP advertisements	GC
lldp med-fast-start-count	Configures how many medFastStart packets are transmitted	GC
lldp notification-interval	Configures the allowed interval for sending SNMP notifications about LLDP changes	GC
lldp refresh-interval	Configures the periodic transmit interval for LLDP advertisements	GC
lldp reinit-delay	Configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down	GC
lldp tx-delay	Configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables	GC
lldp admin-status	Enables LLDP transmit, receive, or transmit and receive mode on the specified port	IC
lldp basic-tlv management-ip-address	Configures an LLDP-enabled port to advertise the management address for this device	IC
lldp basic-tlv port-description	Configures an LLDP-enabled port to advertise its port description	IC
lldp basic-tlv system-capabilities	Configures an LLDP-enabled port to advertise its system capabilities	IC
lldp basic-tlv system-description	Configures an LLDP-enabled port to advertise the system description	IC

Table 142: LLDP Commands (Continued)

Command	Function	Mode
lldp basic-tlv system-name	Configures an LLDP-enabled port to advertise its system name	IC
lldp dot1-tlv proto-ident*	Configures an LLDP-enabled port to advertise the supported protocols	IC
lldp dot1-tlv proto-vid*	Configures an LLDP-enabled port to advertise port related VLAN information	IC
lldp dot1-tlv pvid*	Configures an LLDP-enabled port to advertise its default VLAN ID	IC
lldp dot1-tlv vlan-name*	Configures an LLDP-enabled port to advertise its VLAN name	IC
lldp dot3-tlv link-agg	Configures an LLDP-enabled port to advertise its link aggregation capabilities	IC
lldp dot3-tlv mac-phy	Configures an LLDP-enabled port to advertise its MAC and physical layer specifications	IC
lldp dot3-tlv max-frame	Configures an LLDP-enabled port to advertise its maximum frame size	IC
lldp dot3-tlv poe	Configures an LLDP-enabled port to advertise its Power-over-Ethernet capabilities	IC
lldp med-notification	Enables the transmission of SNMP trap notifications about LLDP-MED changes	IC
lldp med-tlv extpoe	Configures an LLDP-MED-enabled port to advertise its extended Power over Ethernet configuration and usage information	IC
lldp med-tlv inventory	Configures an LLDP-MED-enabled port to advertise its inventory identification details	IC
lldp med-tlv location	Configures an LLDP-MED-enabled port to advertise its location identification details	IC
lldp med-tlv med-cap	Configures an LLDP-MED-enabled port to advertise its Media Endpoint Device capabilities	IC
lldp med-tlv network-policy	Configures an LLDP-MED-enabled port to advertise its network policy configuration	IC
lldp notification	Enables the transmission of SNMP trap notifications about LLDP changes	IC
show lldp config	Shows LLDP configuration settings for all ports	PE
show lldp info local-device	Shows LLDP global and interface-specific configuration settings for this device	PE
show lldp info remote-device	Shows LLDP global and interface-specific configuration settings for remote devices	PE
show lldp info statistics	Shows statistical counters for all LLDP-enabled interfaces	PE

* Vendor-specific options may or may not be advertised by neighboring devices.

lldp

This command enables LLDP globally on the switch. Use the **no** form to disable LLDP.

SYNTAX

[**no**] **lldp**

DEFAULT SETTING
Enabled

COMMAND MODE
Global Configuration

EXAMPLE

```
Console(config)#lldp
Console(config)#
```

lldp holdtime-multiplier

This command configures the time-to-live (TTL) value sent in LLDP advertisements. Use the **no** form to restore the default setting.

SYNTAX

lldp holdtime-multiplier *value*

no lldp holdtime-multiplier

value - Calculates the TTL in seconds based on (holdtime-multiplier * refresh-interval) ≤ 65536 (Range: 2 - 10)

DEFAULT SETTING
Holdtime multiplier: 4
TTL: 4*30 = 120 seconds

COMMAND MODE
Global Configuration

COMMAND USAGE
The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner.

EXAMPLE

```
Console(config)#lldp holdtime-multiplier 10
Console(config)#
```

lldp med-fast-start-count

This command specifies the amount of MED Fast Start LLDPDUs to transmit during the activation process of the LLDP-MED Fast Start mechanism.

SYNTAX

lldp med-fast-start-count *packets*

seconds - Amount of packets. (Range: 1-10 packets; Default: 4 packets)

DEFAULT SETTING
4 packets

COMMAND MODE
Global Configuration

COMMAND USAGE
The MED Fast Start Count parameter is part of the timer which ensures that the LLDP-MED Fast Start mechanism is active for the port. LLDP-MED Fast Start is critical to the timely startup of LLDP, and therefore integral to the rapid availability of Emergency Call Service.

EXAMPLE

```
Console(config)#lldp medfaststartcount 6
Console(config)#
```

lldp notification-interval

This command configures the allowed interval for sending SNMP notifications about LLDP MIB changes. Use the **no** form to restore the default setting.

SYNTAX

lldp notification-interval *seconds*

no lldp notification-interval

seconds - Specifies the periodic interval at which SNMP notifications are sent. (Range: 5 - 3600 seconds)

DEFAULT SETTING
5 seconds

COMMAND MODE
Global Configuration

COMMAND USAGE
- This parameter only applies to SNMP applications which use data stored in the LLDP MIB for network monitoring or management.
- Information about changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

EXAMPLE

```
Console(config)#lldp notification-interval 30
Console(config)#
```

lldp refresh-interval

This command configures the periodic transmit interval for LLDP advertisements. Use the **no** form to restore the default setting.

SYNTAX

lldp refresh-interval *seconds*

no lldp refresh-delay

seconds - Specifies the periodic interval at which LLDP advertisements are sent. (Range: 5 - 32768 seconds)

DEFAULT SETTING

30 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

This attribute must comply with the following rule:
(refresh-interval * holdtime-multiplier) ≤ 65536

EXAMPLE

```
Console(config)#lldp refresh-interval 60
Console(config)#
```

lldp reinit-delay

This command configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down. Use the **no** form to restore the default setting.

SYNTAX

lldp reinit-delay *seconds*

no lldp reinit-delay

seconds - Specifies the delay before attempting to re-initialize LLDP. (Range: 1 - 10 seconds)

DEFAULT SETTING

2 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

When LLDP is re-initialized on a port, all information in the remote systems LLDP MIB associated with this port is deleted.

EXAMPLE

```
Console(config)#lldp reinit-delay 10
Console(config)#
```

lldp tx-delay

This command configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables. Use the **no** form to restore the default setting.

SYNTAX

lldp tx-delay *seconds*

no lldp tx-delay

seconds - Specifies the transmit delay. (Range: 1 - 8192 seconds)

DEFAULT SETTING

2 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

- The transmit delay is used to prevent a series of successive LLDP transmissions during a short period of rapid changes in local LLDP MIB objects, and to increase the probability that multiple, rather than single changes, are reported in each transmission.
- This attribute must comply with the following rule:
  (4 * tx-delay) ≤ refresh-interval

EXAMPLE

```
Console(config)#lldp tx-delay 10
Console(config)#
```

lldp admin-status

This command enables LLDP transmit, receive, or transmit and receive mode on the specified port. Use the **no** form to disable this feature.

SYNTAX

lldp admin-status {**rx-only** | **tx-only** | **tx-rx**}

no lldp admin-status

rx-only - Only receive LLDP PDUs.

tx-only - Only transmit LLDP PDUs.

tx-rx - Both transmit and receive LLDP Protocol Data Units (PDUs).

DEFAULT SETTING
tx-rx

COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp admin-status rx-only
Console(config-if)#
```

lldp basic-tlv management-ip-address

This command configures an LLDP-enabled port to advertise the management address for this device. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp basic-tlv management-ip-address**

DEFAULT SETTING
Enabled

COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE
- The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.
- The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address. The interface number and OID are included to assist SNMP applications to perform network discovery by indicating enterprise specific or other starting points for the search, such as the Interface or Entity MIB.
- Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV.
- Every management address TLV that reports an address that is accessible on a port and protocol VLAN through the particular port should be accompanied by a port and protocol VLAN TLV that indicates the VLAN identifier (VID) associated with the management address reported by this TLV.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv management-ip-address
Console(config-if)#
```

lldp basic-tlv port-description

This command configures an LLDP-enabled port to advertise its port description. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp basic-tlv port-description**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

The port description is taken from the ifDescr object in RFC 2863, which includes information about the manufacturer, the product name, and the version of the interface hardware/software.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv port-description
Console(config-if)#
```

lldp basic-tlv system-capabilities

This command configures an LLDP-enabled port to advertise its system capabilities. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp basic-tlv system-capabilities**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

The system capabilities identifies the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-capabilities
Console(config-if)#
```

lldp basic-tlv system-description

This command configures an LLDP-enabled port to advertise the system description. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp basic-tlv system-description**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

The system description is taken from the sysDescr object in RFC 3418, which includes the full name and version identification of the system's hardware type, software operating system, and networking software.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-description
Console(config-if)#
```

lldp basic-tlv system-name

This command configures an LLDP-enabled port to advertise the system name. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp basic-tlv system-name**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

The system name is taken from the sysName object in RFC 3418, which contains the system's administratively assigned name, and is in turn based on the hostname command.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-name
Console(config-if)#
```

lldp dot1-tlv proto-ident

This command configures an LLDP-enabled port to advertise the supported protocols. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp dot1-tlv proto-ident**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises the protocols that are accessible through this interface.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv proto-ident
Console(config-if)#
```

lldp dot1-tlv proto-vid

This command configures an LLDP-enabled port to advertise port related VLAN information. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp dot1-tlv proto-vid**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises the port-based and protocol-based VLANs configured on this interface (see "Configuring VLAN Interfaces" and "Configuring Protocol-based VLANs").

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv proto-vid
Console(config-if)#
```

lldp dot1-tlv pvid

This command configures an LLDP-enabled port to advertise its default VLAN ID. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp dot1-tlv pvid**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

The port's default VLAN identifier (PVID) indicates the VLAN with which untagged or priority-tagged frames are associated (see the switchport native vlan command).

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv pvid
Console(config-if)#
```

lldp dot1-tlv vlan-name

This command configures an LLDP-enabled port to advertise its VLAN name. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp dot1-tlv vlan-name**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises the name of all VLANs to which this interface has been assigned. See "switchport allowed vlan" and "protocol-vlan protocol-group (Configuring Interfaces)."

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv vlan-name
Console(config-if)#
```

lldp dot3-tlv link-agg

This command configures an LLDP-enabled port to advertise link aggregation capabilities. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp dot3-tlv link-agg**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises link aggregation capabilities, aggregation status of the link, and the 802.3 aggregated port identifier if this interface is currently a link aggregation member.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot3-tlv link-agg
Console(config-if)#
```

lldp dot3-tlv mac-phy

This command configures an LLDP-enabled port to advertise its MAC and physical layer capabilities. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp dot3-tlv mac-phy**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises MAC/PHY configuration/status which includes information about auto-negotiation support/capabilities, and operational Multistation Access Unit (MAU) type.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot3-tlv mac-phy
Console(config-if)#
```

lldp dot3-tlv max-frame

This command configures an LLDP-enabled port to advertise its maximum frame size. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp dot3-tlv max-frame**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

Refer to "Frame Size" for information on configuring the maximum frame size for this switch.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dot3-tlv max-frame
Console(config-if)#
```

lldp dot3-tlv poe

This command configures an LLDP-enabled port to advertise its Power-over-Ethernet (PoE) capabilities. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp dot3-tlv poe**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises Power-over-Ethernet capabilities, including whether or not PoE is supported, currently enabled, if the port pins through which power is delivered can be controlled, the port pins selected to deliver power, and the power class. Note that this device does not support PoE capabilities.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dot3-tlv poe
Console(config-if)#
```

lldp med-notification

This command enables the transmission of SNMP trap notifications about LLDP-MED changes. Use the **no** form to disable LLDP-MED notifications.

SYNTAX

[**no**] **lldp med-notification**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- This option sends out SNMP trap notifications to designated target stations at the interval specified by the lldp notification-interval command. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), the LLDP-MED MIB (ANSI/TIA 1057), or organization-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs.
- SNMP trap destinations are defined using the snmp-server host command.
- Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-notification
Console(config-if)#
```

lldp med-tlv extpoe

This command configures an LLDP-MED-enabled port to advertise and accept Extended Power-over-Ethernet configuration and usage information. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp med-tlv extpoe**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises extended Power-over-Ethernet capability details, such as power availability from the switch, and power state of the switch, including whether the switch is operating from primary or backup power (the Endpoint Device could use this information to decide to enter power conservation mode). Note that this device does not support PoE capabilities.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp medtlv extpoe
Console(config-if)#
```

lldp med-tlv inventory

This command configures an LLDP-MED-enabled port to advertise its inventory identification details. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp med-tlv inventory**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises device details useful for inventory management, such as manufacturer, model, software version and other pertinent information.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp medtlv inventory
Console(config-if)#
```

lldp med-tlv location

This command configures an LLDP-MED-enabled port to advertise its location identification details. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp med-tlv location**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises location identification details.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp medtlv location
Console(config-if)#
```

lldp med-tlv med-cap

This command configures an LLDP-MED-enabled port to advertise its Media Endpoint Device capabilities. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp med-tlv med-cap**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises LLDP-MED TLV capabilities, allowing Media Endpoint and Connectivity Devices to efficiently discover which LLDP-MED related TLVs are supported on the switch.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp medtlv med-cap
Console(config-if)#
```

lldp med-tlv network-policy

This command configures an LLDP-MED-enabled port to advertise its network policy configuration. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp med-tlv network-policy**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises network policy configuration information, aiding in the discovery and diagnosis of VLAN configuration mismatches on a port. Improper network policy configurations frequently result in voice quality degradation or complete service disruption.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp medtlv network-policy
Console(config-if)#
```

lldp notification

This command enables the transmission of SNMP trap notifications about LLDP changes. Use the **no** form to disable LLDP notifications.

SYNTAX

[**no**] **lldp notification**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- This option sends out SNMP trap notifications to designated target stations at the interval specified by the lldp notification-interval command. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), or organization-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs.
- SNMP trap destinations are defined using the snmp-server host command.
- Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission.

An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp notification
Console(config-if)#
```

show lldp config

This command shows LLDP configuration settings for all ports.

SYNTAX

show lldp config [**detail** *interface*]

detail - Shows configuration summary.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show lldp config

LLDP Global Configuation

 LLDP Enable                : Yes
 LLDP Transmit interval     : 30
 LLDP Hold Time Multiplier  : 4
 LLDP Delay Interval        : 2
 LLDP Reinit Delay          : 2
 LLDP Notification Interval : 5
 LLDP MED Fast Start Counts : 4


LLDP Port Configuration
  Interface |AdminStatus NotificationEnabled
  --------- + ----------- -------------------
  Eth 1/1   | Tx-Rx       True
  Eth 1/2   | Tx-Rx       True
  Eth 1/3   | Tx-Rx       True
  Eth 1/4   | Tx-Rx       True
  Eth 1/5   | Tx-Rx       True
.
.
.
Console#show lldp config detail ethernet 1/1

LLDP Port Configuration Detail
```

```
Port : Eth 1/1
Admin Status : Tx-Rx
Notification Enabled : True
Basic TLVs Advertised:
  port-description
  system-name
  system-description
  system-capabilities
  management-ip-address
802.1 specific TLVs Advertised:
 *port-vid
 *vlan-name
 *proto-vlan
 *proto-ident
802.3 specific TLVs Advertised:
 *mac-phy
 *poe
 *link-agg
 *max-frame
MED Configuration:
MED Notification Enabled : True
MED Enabled TLVs Advertised:
 *med-cap
*network-policy
*location
*extPoe
*inventory

Console#
```

show lldp info local-device

This command shows LLDP global and interface-specific configuration settings for this device.

SYNTAX

show lldp info local-device [**detail** *interface*]

detail - Shows configuration summary.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show lldp info local-device

 LLDP Local System Information
  Chassis Type : MAC Address
  Chassis ID   : 00-01-02-03-04-05
  System Name  :
  System Description : 24 10/100 ports and 4 gigabit ports with PoE switch
  System Capabilities Support : Bridge
```

```
  System Capabilities Enable  : Bridge
  Management Address : 192.168.0.101 (IPv4)

 LLDP Port Information
 Interface |PortID Type      PortID            PortDesc
 --------- + --------------- ----------------- --------------------------
 Eth 1/1   |MAC Address      00-01-02-03-04-06 Ethernet Port on unit 1, port 1
 Eth 1/2   |MAC Address      00-01-02-03-04-07 Ethernet Port on unit 1, port 2
 Eth 1/3   |MAC Address      00-01-02-03-04-08 Ethernet Port on unit 1, port 3
 Eth 1/4   |MAC Address      00-01-02-03-04-09 Ethernet Port on unit 1, port 4
.
.
.
Console#show lldp info local-device detail ethernet 1/1

LLDP Port Information Detail

 Port      : Eth 1/1
 Port Type : MAC Address
 Port ID   : 00-01-02-03-04-06
 Port Desc : Ethernet Port on unit 1, port 1

Console#
```

show lldp info remote-device

This command shows LLDP global and interface-specific configuration settings for remote devices attached to an LLDP-enabled port.

SYNTAX

show lldp info remote-device [**detail** *interface*]

detail - Shows configuration summary.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show lldp info remote-device

 LLDP Remote Devices Information

  Interface | ChassisId         PortId            SysName
  --------- + ----------------- ----------------- ---------------------
  Eth 1/1   | 00-01-02-03-04-05 00-01-02-03-04-06

Console#show lldp info remote-device detail ethernet 1/1

 LLDP Remote Devices Information Detail

---------------------------------------------------------------
  Local PortName     : Eth 1/1
  Chassis Type       : MAC Address
```

```
Chassis Id          : 00-01-02-03-04-05
PortID Type         : MAC Address
PortID              : 00-01-02-03-04-06
SysName             :
SysDescr            : 24 10/100 ports and 4 gigabit ports with PoE switch
PortDescr           : Ethernet Port on unit 1, port 1
SystemCapSupported : Bridge
SystemCapEnabled    : Bridge
Remote Management Address :
  00-01-02-03-04-05 (MAC Address)
Remote Port VID : 1
Remote VLAN Name :
  VLAN-1 : DefaultVlan
Remote Protocol Identity (Hex) :
  88-CC
Remote MAC/PHY configuration status :
  Remote port auto-neg supported : Yes
  Remote port auto-neg enabled : Yes
  Remote port auto-neg advertised cap (Hex) : 0000
  Remote port MAU type : 6
Remote Power Via MDI :
  Remote power class : PSE
  Remote power MDI supported : Yes
  Remote power MDI enabled : Yes
  Remote power pair controlable : No
  Remote power pairs : Spare
  Remote power classification : Class1
Remote Link Aggregation :
  Remote link aggregation capable : Yes
  Remote link aggragation enable : No
Remote link aggragation port id : 0
Remote Max Frame Size : 1518

Console#
```

show lldp info statistics

This command shows statistics based on traffic received through all attached LLDP-enabled interfaces.

SYNTAX

show lldp info statistics [**detail** *interface*]

detail - Shows configuration summary.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28/52)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show lldp info statistics

 LLDP Device Statistics

  Neighbor Entries List Last Updated : 2450279 seconds
  New Neighbor Entries Count         : 1
  Neighbor Entries Deleted Count     : 0
  Neighbor Entries Dropped Count     : 0
  Neighbor Entries Ageout Count      : 0

  Port  | NumFramesRecvd NumFramesSent NumFramesDiscarded
  ----- + -------------- ------------- ------------------
  1     | 0              385           0
  2     | 18             17            0
  3     | 0              0             0
  4     | 0              0             0
  5     | 0              0             0
⋮
Console#show lldp info statistics detail ethernet 1/1

 LLDP Port Statistics Detail

  PortName          : Eth 1/1
  Frames Discarded  : 0
  Frames Invalid    : 0
  Frames Received   : 12
  Frames Sent       : 13
  TLVs Unrecognized : 0
  TLVs Discarded    : 0
  Neighbor Ageouts  : 0

Console#
```

43 DOMAIN NAME SERVICE COMMANDS

These commands are used to configure Domain Naming System (DNS) services. Entries can be manually configured in the DNS domain name to IP address mapping table, default domain names configured, or one or more name servers specified to use for domain name to address translation.

Note that domain name services will not be enabled until at least one name server is specified with the ip name-server command and domain lookup is enabled with the ip domain-lookup command.

Table 143: Address Table Commands

Command	Function	Mode
ip domain-list	Defines a list of default domain names for incomplete host names	GC
ip domain-lookup	Enables DNS-based host name-to-address translation	GC
ip domain-name	Defines a default domain name for incomplete host names	GC
ip host	Creates a static IPv4 host name-to-address mapping	GC
ip name-server	Specifies the address of one or more name servers to use for host name-to-address translation	GC
clear dns cache	Clears all entries from the DNS cache	PE
clear host	Deletes entries from the host name-to-address table	PE
show dns	Displays the configuration for DNS services	PE
show dns cache	Displays entries in the DNS cache	PE
show hosts	Displays the static host name-to-address mapping table	PE

ip domain-list

This command defines a list of domain names that can be appended to incomplete host names (i.e., host names passed from a client that are not formatted with dotted notation). Use the **no** form to remove a name from this list.

SYNTAX

[**no**] **ip domain-list** *name*

name - Name of the host. Do not include the initial dot that separates the host name from the domain name. (Range: 1-64 characters)

DEFAULT SETTING

None

COMMAND MODE
Global Configuration

COMMAND USAGE
- Domain names are added to the end of the list one at a time.
- When an incomplete host name is received by the DNS service on this switch, it will work through the domain list, appending each domain name in the list to the host name, and checking with the specified name servers for a match.
- If there is no domain list, the domain name specified with the ip domain-name command is used. If there is a domain list, the default domain name is not used.

EXAMPLE
This example adds two domain names to the current list and then displays the list.

```
Console(config)#ip domain-list sample.com.jp
Console(config)#ip domain-list sample.com.uk
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
Console#
```

RELATED COMMANDS
ip domain-name (929)

ip domain-lookup

This command enables DNS host name-to-address translation. Use the **no** form to disable DNS.

SYNTAX
[**no**] **ip domain-lookup**

DEFAULT SETTING
Disabled

COMMAND MODE
Global Configuration

COMMAND USAGE
- At least one name server must be specified before DNS can be enabled.

- If all name servers are deleted, DNS will automatically be disabled.

EXAMPLE

This example enables DNS and then displays the configuration.

```
Console(config)#ip domain-lookup
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS enabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

RELATED COMMANDS

ip domain-name (929)
ip name-server (931)

ip domain-name

This command defines the default domain name appended to incomplete host names (i.e., host names passed from a client that are not formatted with dotted notation). Use the **no** form to remove the current domain name.

SYNTAX

ip domain-name *name*

no ip domain-name

name - Name of the host. Do not include the initial dot that separates the host name from the domain name. (Range: 1-127 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#ip domain-name sample.com
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS Disabled
Default Domain Name:
    sample.com
```

```
Domain Name List:
Name Server List:
Console#
```

RELATED COMMANDS

ip domain-list (927)
ip name-server (931)
ip domain-lookup (928)

ip host

This command creates a static entry in the DNS table that maps a host name to an IPv4 address. Use the **no** form to remove an entry.

SYNTAX

[**no**] **ip host** *name address1* [*address2* … *address8*]

name - Name of an IPv4 host. (Range: 1-64 characters)

address - Corresponding IPv4 address.

DEFAULT SETTING

No static entries

COMMAND MODE

Global Configuration

COMMAND USAGE

- Servers or other network devices may support one or more connections via multiple IP addresses. If more than one IP address is associated with a host name using this command, a DNS client can try each address in succession, until it establishes a connection with the target device.
- Use the **no ip host** command to clear static entries, or the clear host command to clear dynamic entries.

EXAMPLE

This example maps an IPv4 address to a host name.

```
Console(config)#ip host rd5 192.168.1.55 10.1.0.55
Console(config)#end
Console#show hosts

Hostname
 rd5
Inet address
 192.168.1.55 10.1.0.55
Console#
```

ip name-server

This command specifies the address of one or more domain name servers to use for name-to-address resolution. Use the **no** form to remove a name server from this list.

SYNTAX

[**no**] **ip name-server** *server-address1* [*server-address2* … *server-address6*]

server-address1 - IP address of domain-name server.

server-address2 … *server-address6* - IP address of additional domain-name servers.

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

The listed name servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.

EXAMPLE

This example adds two domain-name servers to the list and then displays the list.

```
Console(config)#ip name-server 192.168.1.55 10.1.0.55
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

RELATED COMMANDS

ip domain-name (929)
ip domain-lookup (928)

clear dns cache

This command clears all entries in the DNS cache.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#clear dns cache
Console#show dns cache
No.     Flag    Type    IP Address      TTL     Domain
------- ------- ------- --------------- ------- --------
Console#
```

clear host

This command deletes dynamic entries from the DNS table.

SYNTAX

clear host {*name* | *}

name - Name of the host. (Range: 1-64 characters)

* - Removes all entries.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

Use the **clear host** command to clear dynamic entries, or the no ip host command to clear static entries.

EXAMPLE

This example clears all dynamic entries from the DNS table.

```
Console(config)#clear host *
Console(config)#
```

show dns

This command displays the configuration of the DNS service.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show dns
Domain Lookup Status:
    DNS Enabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

show dns cache

This command displays entries in the DNS cache.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show dns cache
NO      FLAG    TYPE    IP              TTL     DOMAIN
0       4       Address 199.239.136.200 198     www.times.com
1       4       Address 61.213.189.120   19     a1116.x.akamai.net
2       4       Address 61.213.189.104   19     a1116.x.akamai.net
3       4       CNAME   POINTER TO:2     19     graphics8.nytimes.com
4       4       CNAME   POINTER TO:2     19     graphics478.nytimes.com.edgesui
Console#
```

Table 144: show dns cache - display description

Field	Description
NO	The entry number for each resource record.
FLAG	The flag is always “4” indicating a cache entry and therefore unreliable.
TYPE	This field includes “Address” which specifies the primary name for the owner, and “CNAME” which specifies multiple domain names (or aliases) which are mapped to the same IP address as an existing entry.
IP	The IP address associated with this record.
TTL	The time to live reported by the name server.
DOMAIN	The domain name associated with this record.

show hosts

This command displays the static host name-to-address mapping table.

COMMAND MODE

Privileged Exec

EXAMPLE

Note that a host name will be displayed as an alias if it is mapped to the same address(es) as a previously configured entry.

```
Console#show hosts

Hostname
 rd5
Inet address
 192.168.1.55 10.1.0.55
Console#
```

44 DHCP COMMANDS

These commands are used to configure Dynamic Host Configuration Protocol (DHCP) client functions.

These commands are used to configure Dynamic Host Configuration Protocol (DHCP) client and relay functions. You can configure any VLAN interface to be automatically assigned an IP address via DHCP. This switch can also be configured to relay DHCP client configuration requests to a DHCP server on another network.

Table 145: DHCP Commands

Command Group	Function
DHCP Client	Allows interfaces to dynamically acquire IP address information
DHCP Relay	Relays DHCP requests from local hosts to a remote DHCP server

DHCP CLIENT

Use the commands in this section to allow the switch's VLAN interfaces to dynamically acquire IP address information.

Table 146: DHCP Client Commands

Command	Function	Mode
ip dhcp client class-id	Specifies the DHCP client identifier for an interface	IC
ip dhcp restart	Submits a BOOTP or DHCP client request	PE

ip dhcp client class-id

This command specifies the DCHP client vendor class identifier for the current interface. Use the **no** form to remove this identifier.

SYNTAX

ip dhcp client class-id {**text** *text* | **hex** *hex*}

no ip dhcp client class-id

text - A text string. (Range: 1-32 characters)

hex - A hexadecimal value.

DEFAULT SETTING

None

COMMAND MODE
Interface Configuration (VLAN)

COMMAND USAGE
- This command is used to identify the vendor class and configuration of the switch to the DHCP server, which then uses this information to decide on how to service the client or the type of information to return.
- The general framework for this DHCP option is set out in RFC 2132 (Option 60). This information is used to convey configuration settings or other identification information about a client, but the specific string to use should be supplied by your service provider or network administrator.
- The server should reply with Option 43 information, which encapsulates Option 66 attributes including the TFTP server name and boot file name.

EXAMPLE
```
Console(config)#interface vlan 2
Console(config-if)#ip dhcp client class-id hex 0000e8666572
Console(config-if)#
```

RELATED COMMANDS
ip dhcp restart (936)

ip dhcp restart
This command submits a BOOTP or DHCP client request.

DEFAULT SETTING
None

COMMAND MODE
Privileged Exec

COMMAND USAGE
- This command issues a BOOTP or DHCP client request for any IP interface that has been set to BOOTP or DHCP mode through the ip address command.
- DHCP requires the server to reassign the client's last address if available.
- If the BOOTP or DHCP server has been moved to a different domain, the network portion of the address provided to the client will be based on this new domain.

EXAMPLE

In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart
Console#show ip interface
 IP Address and Netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
 Address Mode:           DHCP
Console#
```

RELATED COMMANDS

ip address (944)

DHCP RELAY

Use the commands in this section to configure the switch to relay DHCP requests from local hosts to a remote DHCP server.

Table 147: DHCP Relay Commands

Command	Function	Mode
ip dhcp relay server	Specifies DHCP server addresses for relay	GC
ip dhcp relay information option	Enables DHCP Option 82 information relay, and specifies the frame format for the remote-id	GC
ip dhcp relay information policy	Specifies how to handle DHCP client requests which already contain Option 82 information	GC
show ip dhcp relay	Displays the configuration settings for DHCP relay service	PE

ip dhcp relay server

This command enables DHCP relay service, and specifies the address of the server to use. Use the **no** form to clear a server address.

SYNTAX

ip dhcp relay server *address-1* [*address-2* ... *address-5*]

no ip dhcp relay server

address - IP address of a DHCP server. (Range: 1-5 addresses)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

USAGE GUIDELINES

- DHCP relay service applies to DHCP client requests received on any configured VLAN, both the management VLAN and non-management VLANs.
- This command is used to configure DHCP relay for host devices attached to the switch. If DHCP relay service is enabled (by specifying the address for at least one DHCP server), and this switch sees a DHCP request broadcast, it inserts its own IP address into the request so the DHCP server will know the subnet where the client is located. Then, the switch forwards the packet to a DHCP server on another network. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client's subnet, and sends a DHCP response back to the DHCP relay agent (i.e., this switch). This switch then passes the DHCP response received from the server to the client.
- You must specify the IP address for at least one DHCP server. Otherwise, the switch's DHCP relay agent will not forward client requests to a DHCP server. Up to five DHCP servers can be specified in order of preference.
- To terminate DHCP relay service, all configured server addresses must be cleared with the **no** form of this command.

EXAMPLE

```
Console(config)#ip dhcp relay server 192.168.10.19
Console(config)#
```

ip dhcp relay information option

This command enables DHCP Option 82 information relay, and specifies the frame format to use for the remote-id when Option 82 information is generated by the switch. Use the **no** form of this command to disable this feature.

SYNTAX

ip dhcp relay information option [**remote-id** {**ip-address** [**encode** {**ascii** | **hex**}] | **mac-address** [**encode** {**ascii** | **hex**}] | **string** *string*}]

no ip dhcp rely information option [**remote-id**]

mac-address - Includes a MAC address field for the relay agent (that is, the MAC address of the switch's CPU).

ip-address - Includes the IP address field for the relay agent (that is, the IP address of the management interface).

encode - Indicates encoding in ASCII or hexadecimal.

string - An arbitrary string inserted into the remote identifier field. (Range: 1-32 characters)

DEFAULT SETTING

Option 82: Disabled
Remote ID: MAC address

COMMAND MODE

Global Configuration

USAGE GUIDELINES

- DHCP provides a relay agent information option for sending information about its DHCP clients or the relay agent itself to the DHCP server. Also known as DHCP Option 82, it allows compatible DHCP servers to use this information when assigning IP addresses, or to set other services or policies for clients.

- When Option 82 is enabled, the requesting client (or an intermediate relay agent that has used the information fields to describe itself) can be identified in the DHCP request packets forwarded by the switch and in reply packets sent back from the DHCP server. Depending on the selected frame format set for the remote-id by this command, this information may specify the MAC address or IP address of the requesting device (that is, the relay agent in this context).

- By default, the relay agent also fills in the Option 82 circuit-id field with information indicating the local interface over which the switch received the DHCP client request, including the stack unit, port, and VLAN ID. This allows DHCP client-server exchange messages to be forwarded between the server and client without having to flood them to the entire VLAN.

  If Option 82 is enabled on the switch, client information will be included in any relayed request packet over any VLAN according to this criteria.

  Table 148: Inserting Option 82 Information - display description

DHCP Relay*	DHCP Option 82	Action
Disabled	Enabled	Circuit-id and remote-id are added to the Option 82 packet, but the gateway Internet address is not included.
Enabled	Enabled	Circuit-id and remote-id are added to the option 82 packet, and the gateway Internet address is included.

  * See ip dhcp relay server.

- DHCP request packets are flooded onto the VLAN which received the request if DHCP relay service is enabled on the switch, and the request packet contains a valid (i.e., non-zero) relay agent address field.

- DHCP reply packets received by the relay agent are handled as follows:

  1. When the relay agent receives a DHCP reply packet with Option 82 information over the management VLAN, it first ensures that the packet is destined for it, and then removes the Option 82 field from the packet.

2. If the DHCP packet's broadcast flag is on, the switch uses the circuit-id information contained in the option 82 information fields to identify the VLAN connected to the requesting client and then broadcasts the DHCP reply packet to this VLAN. If the DHCP packet's broadcast flag is off, the switch uses the circuit-id information in option 82 fields to identify the interface connected to the requesting client and unicasts the reply packet to the client.

- DHCP reply packets are flooded onto the VLAN which received the reply if DHCP relay service is enabled on the switch and any of the following situations apply:
  - The reply packet does not contain Option 82 information.
  - The reply packet contains a valid relay agent address field (that is not the address of this switch), or receives a reply packet with a zero relay agent address through the management VLAN.
  - The reply packet is received on a non-management VLAN.
- Use the ip dhcp relay information policy command to specify how to handle DHCP client request packets which already contain Option 82 information.
- DHCP Snooping Information Option 82 (see page 638) and DHCP Relay Information Option 82 cannot both be enabled at the same time.

EXAMPLE

This example enables Option 82, and sets the frame format of the remote ID for the option to use the MAC address of the switch's CPU.

```
Console(config)#ip dhcp relay information option remote-id mac-address
Console(config)#
```

RELATED COMMANDS

ip dhcp relay information policy (940)
ip dhcp relay server (937)
ip dhcp snooping (636)

ip dhcp relay information policy

This command specifies how to handle client requests which already contain DHCP Option 82 information.

SYNTAX

ip dhcp relay information policy {**drop** | **keep** | **replace**}

drop - Floods the request packet onto the VLAN that received the original request instead of relaying it.

keep - Retains the Option 82 information in the client request, inserts the relay agent's address, and unicasts the packet to the DHCP server.

replace - Replaces the Option 82 information circuit-id and remote-id fields in the client's request with information provided by the relay agent itself, inserts the relay agent's address, and unicasts the packet to the DHCP server.

DEFAULT SETTING
replace

COMMAND MODE
Global Configuration

USAGE GUIDELINES
- Refer to the Usage Guidelines under the ip dhcp relay information option command for information on when Option 82 information is processed by the switch.
- When the Option 82 policy is set to "keep" the original information in the request packet, the frame type specified by the ip dhcp relay information option command is ignored.

EXAMPLE
This example sets the Option 82 policy to keep the client information in the request packet received by the relay agent, and forward this packet on to the DHCP server.

```
Console(config)#ip dhcp relay information policy keep
Console(config)#
```

RELATED COMMANDS
ip dhcp relay information option (938)
ip dhcp relay server (937)
ip dhcp snooping (636)

show ip dhcp relay
This command displays the configuration settings for DHCP relay service.

COMMAND MODE
Privileged Exec

EXAMPLE

```
Console#show ip dhcp-relay
Status of DHCP relay option82:
Insertion of option82 is Enabled.
DHCP option policy :drop.
DHCP relay-server address 192.168.0.4 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
DHCP remote id sub-option : mac address
Console#
```

RELATED COMMANDS
ip dhcp relay server (937)

45 IP INTERFACE COMMANDS

An IP address may be used for management access to the switch over the network. You can manually configure a specific IP address or direct the switch to obtain an IP address from a BOOTP or DHCP server when it is powered on.

An IP address for this switch is obtained via DHCP by default for VLAN 1. You may also need to a establish a default gateway between this device and management stations that exist on another network segment

There are no IP addresses assigned to this switch by default. You must manually configure a new address to manage the switch over your network.

This section describes commands used to configure IP addresses for VLAN interfaces on the switch.

Table 149: Basic IP Configuration Commands

Command	Function	Mode
IP Configuration Commands		
ip address	Sets the IP address for the current interface	IC
ip default-gateway	Defines the default gateway through which this router can reach other subnetworks	GC
ip dhcp restart	Submits a BOOTP or DHCP client request	PE
show ip interface	Displays the IP settings for this device	NE, PE
show ip redirects	Displays the default gateway configured for this device	PE
ping	Sends ICMP echo request packets to another node on the network	NE, PE
ARP Configuration Commands		
clear arp-cache	Deletes all dynamic entries from the ARP cache	PE
show arp	Displays entries in the ARP cache	NE, PE

ip address

This command sets the IP address for the currently selected VLAN interface. Use the **no** form to restore the default IP address.

SYNTAX

ip address {*ip-address netmask* | **bootp** | **dhcp**}
[**default-gateway** *gateway*]

no ip address

ip-address - IP address

netmask - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.

bootp - Obtains IP address from BOOTP.

dhcp - Obtains IP address from DHCP.

gateway - IP address of the default gateway

DEFAULT SETTING

IP Address: 192.168.1.10
Subnet Mask: 255.255.255.0

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- An IP address must be assigned to this device to gain management access over the network. A specific IP address can be manually configured, or the switch can be directed to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Anything other than this format is not be accepted by the configuration program.

- If **bootp** or **dhcp** options are selected, the system will immediately start broadcasting service requests for all VLANs configured to obtain address assignments through BOOTP or DHCP. IP is enabled but will not function until a BOOTP or DHCP reply has been received. Requests are broadcast periodically by the switch in an effort to learn its IP address. (BOOTP and DHCP values can include the IP address, default gateway, and subnet mask). If the DHCP/BOOTP server is slow to respond, you may need to use the ip dhcp restart command to re-start broadcasting service requests, or reboot the switch.

NOTE: Only one VLAN interface can be assigned an IP address (the default is VLAN 1). This defines the management VLAN, the only VLAN through which you can gain management access to the switch. If you assign an IP address to any other VLAN, the new IP address overrides the original IP address and this becomes the new management VLAN.

- A default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the switch.

- A gateway must be defined if the management station is located in a different IP segment.

EXAMPLE

In the following example, the device is assigned an address in VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

RELATED COMMANDS

ip dhcp restart (936)
show ip redirects (946)

ip default-gateway

This command establishes a static route between this switch and devices that exist on another network segment. Use the **no** form to remove a default gateway.

SYNTAX

ip default-gateway *gateway*

no ip default-gateway

gateway - IP address of the default gateway

DEFAULT SETTING

No default gateway is established.

COMMAND MODE

Global Configuration

COMMAND USAGE

- A default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the switch.
- A gateway must be defined if the management station is located in a different IP segment.

EXAMPLE

The following example defines a default gateway for this device:

```
Console(config)#ip default-gateway 10.1.1.254
Console(config)#
```

RELATED COMMANDS

show ip redirects (946)

show ip interface

This command displays the settings of an IP interface.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
Console#show ip interface
 IP Address and Netmask:  192.168.0.2 255.255.255.0 on VLAN 1,
 Address Mode:            DHCP
Console#
```

RELATED COMMANDS

ip address (944)

show ip redirects

This command shows the default gateway configured for this device.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip redirects
IP default gateway 10.1.0.254
Console#
```

RELATED COMMANDS

ip default-gateway (945)

ping

This command sends ICMP echo request packets to another node on the network.

SYNTAX

ping *host* [**count** *count*] [**size** *size*]

host - IP address or IP alias of the host.

count - Number of packets to send. (Range: 1-16)

size - Number of bytes in a packet. (Range: 32-512)
The actual packet size will be eight bytes larger than the size specified because the router adds header information.

DEFAULT SETTING

count: 5
size: 32 bytes

COMMAND MODE
Normal Exec, Privileged Exec

COMMAND USAGE
- Use the ping command to see if another site on the network can be reached.
- The following are some results of the **ping** command:
  - *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.
  - *Destination does not respond* - If the host does not respond, a "timeout" appears in ten seconds.
  - *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
  - *Network or host unreachable* - The gateway found no corresponding entry in the route table.
- When pinging a host name, be sure the DNS server has been enabled (see page 928). If necessary, local devices can also be specified in the DNS static host table (see page 930).

EXAMPLE
```
Console#ping 10.1.0.9
Type ESC to abort.
PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 5 seconds
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 0 ms
Ping statistics for 10.1.0.9:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
 Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms
Console#
```

RELATED COMMANDS
interface (682)

clear arp-cache

This command deletes all dynamic entries from the Address Resolution Protocol (ARP) cache.

COMMAND MODE

Privileged Exec

EXAMPLE

This example clears all dynamic entries in the ARP cache.

```
Console#clear arp-cache
This operation will delete all the dynamic entries in ARP Cache.
Are you sure to continue this operation (y/n)?y
Console#
```

show arp

This command displays entries in the Address Resolution Protocol (ARP) cache.

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

This command displays information about the ARP cache. It shows each cache entry, including the IP address, MAC address, type (static, dynamic, other), and VLAN interface. Note that entry type "other" indicates local addresses for this switch.

EXAMPLE

This example displays all entries in the ARP cache.

```
Console#show arp

IP Address      MAC Address       Type      Interface
--------------- ----------------- --------- -----------
10.1.0.0        FF-FF-FF-FF-FF-FF other     VLAN1
10.1.0.254      00-00-AB-CD-00-00 other     VLAN1
10.1.0.255      FF-FF-FF-FF-FF-FF other     VLAN1
123.20.10.123   02-10-20-30-40-50 static    VLAN2
145.30.20.23    09-50-40-30-20-10 dynamic   VLAN3

Total entry : 5
Console#
```

Section IV

Appendices

This section provides additional information and includes these items:

A SOFTWARE SPECIFICATIONS

SOFTWARE FEATURES

MANAGEMENT AUTHENTICATION	Local, RADIUS, TACACS+, Port Authentication (802.1X), AAA, HTTPS, SSH, IP Filter
CLIENT ACCESS CONTROL	Access Control Lists (IP/MAC; 1000 rules per system), Port Authentication (802.1X), MAC Authentication, Web Authentication, Port Security, ARP Inspection, DHCP Snooping, IP Source Guard
PORT CONFIGURATION	100BASE-TX: 10/100 Mbps, half/full duplex 1000BASE-T: 10/100 Mbps at half/full duplex, 1000 Mbps at full duplex 1000BASE-SX/LX/LH - 1000 Mbps at full duplex (SFP)
FLOW CONTROL	Full Duplex: IEEE 802.3-2005 Half Duplex: Back pressure
STORM CONTROL	Broadcast, multicast, or unicast traffic throttled above a critical threshold
PORT MIRRORING	One or more source ports to one destination port
RATE LIMITS	Input/Output Limits Range configured per port
PORT TRUNKING	Static trunks (Cisco EtherChannel compliant) Dynamic trunks (Link Aggregation Control Protocol)
SPANNING TREE ALGORITHM	Spanning Tree Protocol (STP, IEEE 802.1D-2004) Rapid Spanning Tree Protocol (RSTP, IEEE 802.1D-2004) Multiple Spanning Tree Protocol (MSTP, IEEE 802.1D-2004)

VLAN SUPPORT	Up to 255 groups; port-based or tagged (802.1Q), protocol-based, private VLANs, voice VLANs, IP subnet, MAC-based, GVRP for automatic VLAN learning
CLASS OF SERVICE	Supports four levels of priority Strict or Weighted Round Robin (WRR) Layer 3/4 priority mapping: IP DSCP
QUALITY OF SERVICE	DiffServ supports class maps, policy maps, and service policies
MULTICAST FILTERING	IGMP Snooping (IPv4) MLD Snooping (IPv6) Multicast VLAN Registration
ADDITIONAL FEATURES	BOOTP Client DHCP Client DHCP Snooping DNS Client, Proxy IP Source Guard LLDP (Link Layer Discover Protocol) RMON (Remote Monitoring, groups 1,2,3,9) SMTP Email Alerts SNMP (Simple Network Management Protocol) SNTP (Simple Network Time Protocol)

MANAGEMENT FEATURES

IN-BAND MANAGEMENT	Telnet, web-based HTTP or HTTPS, SNMP manager, or Secure Shell
OUT-OF-BAND MANAGEMENT	RS-232 DB-9 console port
SOFTWARE LOADING	HTTP, FTP or TFTP in-band, or XModem out-of-band
SNMP	Management access via MIB database Trap management to specified hosts

RMON Groups 1, 2, 3, 9 (Statistics, History, Alarm, Event)

STANDARDS

IEEE 802.1AB Link Layer Discovery Protocol
IEEE 802.1D-2004 Spanning Tree Algorithm and traffic priorities
Spanning Tree Protocol
Rapid Spanning Tree Protocol
Multiple Spanning Tree Protocol
IEEE 802.1p Priority tags
IEEE 802.1Q VLAN
IEEE 802.1v Protocol-based VLANs
IEEE 802.1X Port Authentication
IEEE 802.3-2005
Ethernet, Fast Ethernet, Gigabit Ethernet
Link Aggregation Control Protocol (LACP)
Full-duplex flow control (ISO/IEC 8802-3)
IEEE 802.3ac VLAN tagging
DHCP Client (RFC 2131)
FTP (RFC 959)RIP (RFC 1058)
DHCP Options (RFC 2132)
HTTPS
ICMP (RFC 792)
IGMP (RFC 1112)
IGMPv2 (RFC 2236)
IGMPv3 (RFC 3376) - partial support
IPv4 IGMP (RFC 3228)
RADIUS+ (RFC 2618)
RMON (RFC 2819 groups 1,2,3,9)
SNMP (RFC 1157)
SNMPv2c (RFC 1901, 2571)
SNMPv3 (RFC DRAFT 2273, 2576, 3410, 3411, 3413, 3414, 3415)
SNTP (RFC 2030)
SSH (Version 2.0)
TELNET (RFC 854, 855, 856)
TFTP (RFC 1350)

MANAGEMENT INFORMATION BASES

Bridge MIB (RFC 1493)
Differentiated Services MIB (RFC 3289)
DNS Resolver MIB (RFC 1612)

Entity MIB (RFC 2737)
Ether-like MIB (RFC 3635)
Extended Bridge MIB (RFC 2674)
Extensible SNMP Agents MIB (RFC 2742)
Forwarding Table MIB (RFC 2096)
IGMP MIB (RFC 2933)
Interface Group MIB (RFC 2233)
Interfaces Evolution MIB (RFC 2863)
IP Multicasting related MIBs
Link Aggregation MIB (IEEE 802.3ad)
MAU MIB (RFC 3636)
MIB II (RFC 1213)
P-Bridge MIB (RFC 2674P)
Port Access Entity MIB (IEEE 802.1X)
Port Access Entity Equipment MIB
Private MIB
Q-Bridge MIB (RFC 2674Q)
QinQ Tunneling (IEEE 802.1ad Provider Bridges)
Quality of Service MIB
RIP1 MIB (RFC 1058)
RIP2 MIB (RFC 2453)
OSPF MIB (RFC 1850)
RADIUS Accounting Server MIB (RFC 2621)
RADIUS Authentication Client MIB (RFC 2621)
RMON MIB (RFC 2819)
RMON II Probe Configuration Group (RFC 2021, partial implementation)
SNMP Community MIB (RFC 3584)
SNMP Framework MIB (RFC 3411)
SNMP-MPD MIB (RFC 3412)
SNMP Target MIB, SNMP Notification MIB (RFC 3413)
SNMP User-Based SM MIB (RFC 3414)
SNMP View Based ACM MIB (RFC 3415)
SNMPv2 IP MIB (RFC 2011)
TACACS+ Authentication Client MIB
TCP MIB (RFC 2012)
Trap (RFC 1215)
UDP MIB (RFC 2013)

B TROUBLESHOOTING

PROBLEMS ACCESSING THE MANAGEMENT INTERFACE

Table 150: Troubleshooting Chart

Symptom	Action
Cannot connect using Telnet, web browser, or SNMP software	◆ Be sure the switch is powered up. ◆ Check network cabling between the management station and the switch. ◆ Check that you have a valid network connection to the switch and that the port you are using has not been disabled. ◆ Be sure you have configured the VLAN interface through which the management station is connected with a valid IP address, subnet mask and default gateway. ◆ Be sure the management station has an IP address in the same subnet as the switch's IP interface to which it is connected. ◆ If you are trying to connect to the switch via the IP address for a tagged VLAN group, your management station, and the ports connecting intermediate switches in the network, must be configured with the appropriate tag. ◆ If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time.
Cannot connect using Secure Shell	◆ If you cannot connect using SSH, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time. ◆ Be sure the control parameters for the SSH server are properly configured on the switch, and that the SSH client software is properly configured on the management station. ◆ Be sure you have generated both an RSA and DSA public key on the switch, exported this key to the SSH client, and enabled SSH service. ◆ Be sure you have set up an account on the switch for each SSH user, including user name, authentication level, and password. ◆ Be sure you have imported the client's public key to the switch (if public key authentication is used).
Cannot access the on-board configuration program via a serial port connection	◆ Be sure you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity, and the baud rate set to 9600 bps. ◆ Check that the null-modem serial cable conforms to the pin-out connections provided in the Installation Guide.
Forgot or lost the password	◆ Contact your local distributor.

USING SYSTEM LOGS

If a fault does occur, refer to the Installation Guide to ensure that the problem you encountered is actually caused by the switch. If the problem appears to be caused by the switch, follow these steps:

1. Enable logging.
2. Set the error messages reported to include all categories.
3. Enable SNMP.
4. Enable SNMP traps.
5. Designate the SNMP host that is to receive the error messages.
6. Repeat the sequence of commands or other actions that lead up to the error.
7. Make a list of the commands or circumstances that led to the fault. Also make a list of any error messages displayed.
8. Set up your terminal emulation software so that it can capture all console output to a file. Then enter the "show tech-support" command to record all system settings in this file.
9. Contact your distributor's service engineer, and send a detailed description of the problem, along with the file used to record your system settings.

For example:

```
Console(config)#logging on
Console(config)#logging history flash 7
Console(config)#snmp-server host 192.168.1.23
⋮
```

GLOSSARY

ACL Access Control List. ACLs can limit network traffic and restrict access to certain users or devices by checking each packet for certain IP or MAC (i.e., Layer 2) information.

ARP Address Resolution Protocol converts between IP addresses and MAC (hardware) addresses. ARP is used to locate the MAC address corresponding to a given IP address. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next.

BOOTP Boot Protocol. BOOTP is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

CoS Class of Service is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence bit, or DSCP priority bit.

DHCP Dynamic Host Control Protocol. Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

DHCP OPTION 82 A relay option for sending information about the requesting client (or an intermediate relay agent) in the DHCP request packets forwarded by the switch and in reply packets sent back from the DHCP server. This information can be used by DHCP servers to assign fixed IP addresses, or set other services or policies for clients.

DHCP SNOOPING A technique used to enhance network security by snooping on DHCP server messages to track the physical location of hosts, ensure that hosts only use the IP addresses assigned to them, and ensure that only authorized DHCP servers are accessible.

DIFFSERV Differentiated Services provides quality of service on large networks by employing a well-defined set of building blocks from which a variety of aggregate forwarding behaviors may be built. Each packet carries information (DS byte) used by each hop to give it a particular forwarding treatment, or per-hop behavior, at each network node. DiffServ allocates different levels of service to users on the network with mechanisms such as traffic meters, shapers/droppers, packet markers at the boundaries of the network.

DNS Domain Name Service. A system used for translating host names for network nodes into IP addresses.

DSCP Differentiated Services Code Point Service. DSCP uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.

EAPOL Extensible Authentication Protocol over LAN. EAPOL is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A user name and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1X Port Authentication standard.

FILE TRANSFER PROTOCOL (FTP) A TCP/IP protocol commonly used for software downloads.

GARP Generic Attribute Registration Protocol. GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.

GMRP Generic Multicast Registration Protocol. GMRP allows network devices to register end stations with multicast groups. GMRP requires that any participating network devices or end stations comply with the IEEE 802.1p standard.

GVRP GARP VLAN Registration Protocol. Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

IEEE 802.1D Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.1P An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

IEEE 802.1S An IEEE standard for the Multiple Spanning Tree Protocol (MSTP) which provides independent spanning trees for VLAN groups.

IEEE 802.1W An IEEE standard for the Rapid Spanning Tree Protocol (RSTP) which reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard. (Now incorporated in IEEE 802.1D-2004)

IEEE 802.1X Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

IEEE 802.3AC Defines frame extensions for VLAN tagging.

IEEE 802.3X Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links. (Now incorporated in IEEE 802.3-2002)

IGMP Internet Group Management Protocol. A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast switch/router on a given subnetwork, one of the devices is made the "querier" and assumes responsibility for keeping track of group membership.

IGMP QUERY On each subnetwork, one IGMP-capable device will act as the querier — that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

IGMP PROXY Proxies multicast group membership information onto the upstream interface based on IGMP messages monitored on downstream interfaces, and forwards multicast traffic based on that information. There is no need for multicast routing protocols in an simple tree that uses IGMP Proxy.

IGMP SNOOPING Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

IN-BAND MANAGEMENT Management of the network from a station attached directly to the network.

IP MULTICAST FILTERING A process whereby this switch can pass multicast traffic along to participating hosts.

IP PRECEDENCE The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The eight values are mapped one-to-one to the Class of Service categories by default, but may be configured differently to suit the requirements for specific network applications.

LACP Link Aggregation Control Protocol. Allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

LAYER 2 Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

LINK AGGREGATION *See Port Trunk.*

LLDP Link Layer Discovery Protocol is used to discover basic information about neighboring devices in the local broadcast domain by using periodic broadcasts to advertise information such as device identification, capabilities and configuration settings.

MD5 MD5 Message-Digest is an algorithm that is used to create digital signatures. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

MIB Management Information Base. An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

MSTP Multiple Spanning Tree Protocol can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group.

MULTICAST SWITCHING A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

MVR Multicast VLAN Registration is a method of using a single network-wide multicast VLAN to transmit common services, such as such as television channels or video-on-demand, across a service-provider's network. MVR simplifies the configuration of multicast services by using a common VLAN for distribution, while still preserving security and data isolation for subscribers residing in both the MVR VLAN and other standard or private VLAN groups.

NTP Network Time Protocol provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

OUT-OF-BAND MANAGEMENT Management of the network from a station not attached to the network.

PORT AUTHENTICATION *See IEEE 802.1X*.

PORT MIRRORING A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

PORT TRUNK Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

PRIVATE VLANS Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports.

QINQ QinQ tunneling is designed for service providers carrying traffic for multiple customers across their networks. It is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs.

QOS Quality of Service. QoS refers to the capability of a network to provide better service to selected traffic flows using features such as data prioritization, queuing, congestion avoidance and traffic shaping. These features effectively provide preferential treatment to specific flows either by raising the priority of one flow or limiting the priority of another flow.

RADIUS Remote Authentication Dial-in User Service. RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

RMON Remote Monitoring. RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

RSTP Rapid Spanning Tree Protocol. RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.

SMTP Simple Mail Transfer Protocol is a standard host-to-host mail transport protocol that operates over TCP, port 25.

SNMP Simple Network Management Protocol. The application protocol in the Internet suite of protocols which offers network management services.

SNTP Simple Network Time Protocol allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

SSH Secure Shell is a secure replacement for remote access functions, including Telnet. SSH can authenticate users with a cryptographic key, and encrypt data connections between management clients and the switch.

STA Spanning Tree Algorithm is a technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

TACACS+ Terminal Access Controller Access Control System Plus. TACACS+ is a logon authentication protocol that uses software running on a central server to control access to TACACS-compliant devices on the network.

TCP/IP Transmission Control Protocol/Internet Protocol. Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

TELNET Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

TFTP Trivial File Transfer Protocol. A TCP/IP protocol commonly used for software downloads.

UDP User Datagram Protocol. UDP provides a datagram mode for packet-switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

UTC Universal Time Coordinate. UTC is a time scale that couples Greenwich Mean Time (based solely on the Earth's rotation rate) with highly accurate atomic time. The UTC does not have daylight saving time.

VLAN Virtual LAN. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

XMODEM A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

COMMAND LIST

E

F

G

H

I

J

L

M

N

P

Q

R

S

T

U

V

W

INDEX

NUMERICS

A

B

C

D

E

M

N

P

Q

R

S

T

U

V

W