Software Management Guide

NXA-ENET24

Managed Ethernet Switches

Network/Communication

Last Revised: 3/19/2010

AMX Limited Warranty and Disclaimer

This Limited Warranty and Disclaimer extends only to products purchased directly from AMX or an AMX Authorized Partner which include AMX Dealers, Distributors, VIP's or other AMX authorized entity.

AMX warrants its products to be free of defects in material and workmanship under normal use for three (3) years from the date of purchase, with the following exceptions:

- Electroluminescent and LCD Control Panels are warranted for three (3) years, except for the display and touch overlay components are warranted for a period of one (1) year.
- Disk drive mechanisms, pan/tilt heads, power supplies, and MX Series products are warranted for a period of one (1) year.
- AMX lighting products are guaranteed to switch on and off any load that is properly connected to our lighting products, as long as the AMX lighting products are under warranty. AMX also guarantees the control of dimmable loads that are properly connected to our lighting products. The dimming performance or quality there of is not guaranteed, impart due to the random combinations of dimmers, lamps and ballasts or transformers.
- AMX software is warranted for a period of ninety (90) days.
- Batteries and incandescent lamps are not covered under the warranty.
- AMX AutoPatch Epica, Modula, Modula Series4, Modula CatPro Series and 8Y-3000 product models will be free of defects in materials and manufacture at the time of sale and will remain in good working order for a period of three (3) years following the date of the original sales invoice from AMX. The three-year warranty period will be extended to the life of the product (Limited Lifetime Warranty) if the warranty card is filled out by the dealer and/or end user and returned to AMX so that AMX receives it within thirty (30) days of the installation of equipment but no later than six (6) months from original AMX sales invoice date. The life of the product extends until five (5) years after AMX ceases manufacturing the product model. The Limited Lifetime Warranty applies to products in their original installation only. If a product is moved to a different installation, the Limited Lifetime Warranty will no longer apply, and the product warranty will instead be the three (3) year Limited Warranty.

All products returned to AMX require a Return Material Authorization (RMA) number. The RMA number is obtained from the AMX RMA Department. The RMA number must be clearly marked on the outside of each box. The RMA is valid for a 30-day period. After the 30-day period the RMA will be cancelled. Any shipments received not consistent with the RMA, or after the RMA is cancelled, will be refused. AMX is not responsible for products returned without a valid RMA number.

AMX is not liable for any damages caused by its products or for the failure of its products to perform. This includes any lost profits, lost savings, incidental damages, or consequential damages. AMX is not liable for any claim made by a third party or by an AMX Authorized Partner for a third party.

This Limited Warranty does not apply to (a) any AMX product that has been modified, altered or repaired by an unauthorized agent or improperly transported, stored, installed, used, or maintained; (b) damage caused by acts of nature, including flood, erosion, or earthquake; (c) damage caused by a sustained low or high voltage situation or by a low or high voltage disturbance, including brownouts, sags, spikes, or power outages; or (d) damage caused by war, vandalism, theft, depletion, or obsolescence.

This limitation of liability applies whether damages are sought, or a claim is made, under this warranty or as a tort claim (including negligence and strict product liability), a contract claim, or any other claim. This limitation of liability cannot be waived or amended by any person. This limitation of liability will be effective even if AMX or an authorized representative of AMX has been advised of the possibility of any such damages. This limitation of liability, however, will not apply to claims for personal injury.

Some states do not allow a limitation of how long an implied warranty last. Some states do not allow the limitation or exclusion of incidental or consequential damages for consumer products. In such states, the limitation or exclusion of the Limited Warranty may not apply. This Limited Warranty gives the owner specific legal rights. The owner may also have other rights that vary from state to state. The owner is advised to consult applicable state laws for full determination of rights.

EXCEPT AS EXPRESSLY SET FORTH IN THIS WARRANTY, AMX MAKES NO OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. AMX EXPRESSLY DISCLAIMS ALL WARRANTIES NOT STATED IN THIS LIMITED WARRANTY. ANY IMPLIED WARRANTIES THAT MAY BE IMPOSED BY LAW ARE LIMITED TO THE TERMS OF THIS LIMITED WARRANTY. EXCEPT AS OTHERWISE LIMITED BY APPLICABLE LAW, AMX RESERVES THE RIGHT TO MODIFY OR DISCONTINUE DESIGNS, SPECIFICATIONS, WARRANTIES, PRICES, AND POLICIES WITHOUT NOTICE.

Table of Contents

Introduction

The NXA-ENET24 Fast Ethernet switch is specifically designed to protect the video streams coming from AMX's MAX units to the Audio Video Modules (AVM). Standard switches will reduce bandwidth from all applications when there is heavy data traffic passing through the switch. For streaming audio and video applications this will cause skipping and jitter in the audio and video feeds. This is unacceptable for AMX's applications. As a result, AMX has designed the NXA-ENET24 to protect the A/V streams when heavy data traffic occurs. Bandwidth is reduced from other applications such as file transfer, e-mail and web surfing only when during heavy data traffic events.

The NXA-ENET24 also provides a full 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.

The NXA-ENET24 PoE's 24 10/100 Mbps ports support the IEEE 802.3af Power-over-Ethernet (PoE) standard that enables DC power to be supplied to attached devices over the unused pairs of wires in the connecting Ethernet cable.

Key Features

Key Features

Feature	Description
Power over Ethernet	Powers attached devices using IEEE 802.3af Power over Ethernet (PoE)
Configuration Backup and Restore	Backup to TFTP server
Authentication	Console, Telnet – User name / password, RADIUS, TACACS+ Telnet – SSH SNMP – Community strings, IP address filtering Port – IEEE 802.1x, MAC address filtering
Access Control Lists	Supports up to 32 IP or MAC ACLs
Access Control Lists	Supports up to 32 IP or MAC ACLs
DHCP Client, Relay	Supported
DNS Server	Supported
Port Configuration	Speed, duplex mode and flow control
Rate Limiting	Input and output rate limiting per port
Port Mirroring	One or more ports mirrored to single analysis port
Port Trunking	Supports port trunking using either static or dynamic trunking (LACP)
Broadcast Storm Control	Supported
Static Address	Up to 8K MAC addresses in the forwarding table, 128 static entries in ARP cache
IEEE 802.1D Bridge	Supports dynamic data switching and address learning
Store-and-Forward Switching	Supported to ensure wire-speed switching while eliminating bad frames
Spanning Tree Protocol	Supports standard STP and Rapid Spanning Tree Protocol (RSTP)
Virtual LANs	Up to 255 using IEEE 802.1Q, port-based, or private VLANs
Traffic Prioritization	Default port priority, traffic class map, queue scheduling, IP Precedence, or Differentiated Services Code Point (DSCP), and TCP/UDP Port
IP Routing	Routing Information Protocol (RIP), Open Shortest Path First (OSPF), static routes
ARP	Static and dynamic address configuration, proxy ARP
Multicast Filtering	Supports IGMP snooping and query for Layer 2, and IGMP for Layer 3
Multicast Routing	Supports DVMRP and PIM-DM

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. Broadcast storm suppression prevents broadcast traffic storms from engulfing the network. Port-based VLANs 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 and routing 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 a TFTP server, and later download this file to restore the switch configuration settings.

- **Authentication** – This switch authenticates management access via the console port or Telnet. 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 the 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 SSH for secure management access over a Telnet-equivalent connection, IP address filtering for SNMP/Telnet management access, and MAC address filtering for port access.
- **Access Control Lists** – ACLs provide packet filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or any frames (based on MAC address or Ethernet type). ACLs can by used to improve performance by blocking unnecessary network traffic or to implement security controls by restricting access to specific network resources or protocols.
- **Access Control Lists** – ACLs provide packet filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or any frames (based on MAC address or Ethernet type). ACLs can by used to improve performance by blocking unnecessary network traffic or to implement security controls by restricting access to specific network resources or protocols.
- **DHCP Server and DHCP Relay** – Since DHCP uses a broadcast mechanism, a DHCP server and its client must physically reside on the same subnet. Since it is not practical to have a DHCP server on every subnet, DHCP Relay is also supported to allow dynamic configuration of local clients from a DHCP server located in a different network.
- **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 the 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.
- **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. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.
- **Port Mirroring** – The switch can unobtrusively mirror traffic from any port 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 IEEE 802.3ad Link Aggregation Control Protocol (LACP). 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 one trunk with two Gigabit optional module ports.
- **Broadcast Storm Control** – Broadcast suppression prevents broadcast traffic from overwhelming the network. When enabled on a port, the level of broadcast traffic passing through the port is restricted. If broadcast 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.

- **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 8 MB for frame buffering. This buffer can queue packets awaiting transmission on congested networks.
- **Spanning Tree Protocol** – The switch supports these spanning tree protocols:

  Spanning Tree Protocol (STP, IEEE 802.1D) – This protocol adds a level of fault tolerance by allowing two or more redundant connections to be created between a pair of LAN segments. 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 802.1w) – This protocol reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard. It is intended as a complete replacement for STP, but can still inter-operate with switches running the older standard by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from attached devices.
- **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 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, except where a connection is explicitly defined via the switch’s routing service.
  - 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.
- **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 (video) and best-effort data (e-mail).

  This switch also supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic can be prioritized based on the priority bits in the IP frame’s Type of Service (ToS) octet or the number of the TCP/UDP port. 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.
- **IP Routing** – The switch provides Layer 3 IP routing. To maintain a high rate of throughput, the switch forwards all traffic passing within the same segment, and routes only traffic that passes between different subnetworks. The wire-speed routing provided by this switch lets you easily link network segments or VLANs together without having to deal with the bottlenecks or configuration hassles normally associated with conventional routers.

  Routing for unicast traffic is supported with the Routing Information Protocol (RIP) and the Open Shortest Path First (OSPF) protocol.

- RIP – This protocol uses a distance-vector approach to routing. Routes are determined on the basis of minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost.
- OSPF – This approach uses a link state routing protocol to generate a shortest-path tree, then builds up its routing table based on this tree. OSPF produces a more stable network because the participating routers act on network changes predictably and simultaneously, converging on the best route more quickly than RIP.

- **Address Resolution Protocol** – The switch uses ARP and Proxy ARP to convert between IP addresses and MAC (i.e., hardware) addresses. This switch supports conventional ARP, which locates 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. You can configure either static or dynamic entries in the ARP cache.

  Proxy ARP allows hosts that do not support routing to determine the MAC address of a device on another network or subnet. When a host sends an ARP request for a remote network, the switch checks to see if it has the best route. If it does, it sends its own MAC address to the host. The host then sends traffic for the remote destination via the switch, which uses its own routing table to reach the destination on the other network.
- **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 at Layer 2 and IGMP at Layer 3 to manage multicast group registration.
- **Multicast Routing** – Routing for multicast packets is supported by the Distance Vector Multicast Routing Protocol (DVMRP) and Protocol-Independent Multicasting - Dense Mode (PIM-DM). These protocols work in conjunction with IGMP to filter and route multicast traffic. DVMRP is a more comprehensive implementation that maintains its own routing table, but is gradually being replacing by most network managers with PIM, Dense Mode and Sparse Mode. PIM is a very simple protocol that uses the routing table of the unicast routing protocol enabled on an interface. Dense Mode is designed for areas where the probability of multicast clients is relatively high, and the overhead of frequent flooding is justified. While Sparse mode is designed for network areas, such as the Wide Area Network, where the probability of multicast clients is low. This switch currently supports DVMRP and PIM-DM.

Software Specifications

Software Specifications	
Software Features	
Authentication:	Local, RADIUS, TACACS, Port (802.1x), HTTPS, SSH, Port Security
Access Control Lists:	IP, MAC (up to 32 lists)
POE:	Power Over Ethernet
SNMPv3:	• Management access via MIB database • Trap management to specified hosts
DHCP:	Client, Relay
Port Configuration:	• 100BASE-TX: 10/100 Mbps, half/full duplex • 1000BASE-T: 10/100/1000 Mbps, half/full duplex • 1000BASE-X: 1000 Mbps, full duplex
Flow Control:	• Full Duplex: IEEE 802.3x • Half Duplex: Back pressure
Broadcast Storm Control:	Traffic throttled above a critical threshold
Port Mirroring:	Multiple source ports, one destination port
Rate Limits:	• Input limit • Output limit • Range (configured per port)

Software Specifications (Cont.)	
Software Features (Cont.)	
Port Trunking:	• Static trunks (Cisco EtherChannel compliant) • Dynamic trunks (Link Aggregation Control Protocol)
Spanning Tree Protocol:	• Spanning Tree Protocol (STP, IEEE 802.1D) • Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w)
VLAN Support:	• Up to 255 groups; port-based, protocol-based, or tagged (802.1Q), • GVRP for automatic VLAN learning, private VLANs
Class of Service:	Supports four levels of priority and Weighted Round Robin Queueing (which can be configured by VLAN tag or port), Layer 3/4 priority mapping: • IP Port • IP Precedence • IP DSCP
Multicast Filtering:	• IGMP Snooping (Layer 2) • IGMP (Layer 3)
Multicast Routing:	• DVMRP • PIM-DM
IP Routing:	ARP, Proxy ARP Static routes: • RIP • RIPv2 • OSPFv2 dynamic routing
Additional Features:	• BOOTP client • CIDR (Classless Inter-Domain Routing) • SNTP (Simple Network Time Protocol) • SNMP (Simple Network Management Protocol) • RMON (Remote Monitoring, groups 1,2,3,9) • SMTP Email Alerts
Management Features	
In-Band Management:	• Telnet • Web-based HTTP or HTTPS • SNMP manager • Secure Shell
Out-of-Band Management:	RS-232 DB-9 console port
Software Loading:	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)

Software Specifications (Cont.)	
Standards:	• IEEE 802.3 Ethernet, • IEEE 802.3u Fast Ethernet • IEEE 802.3x full-duplex flow control (ISO/IEC 8802-3) • IEEE 802.3z Gigabit Ethernet, • IEEE 802.3ab 1000BASE-T • IEEE 802.3ac VLAN tagging • IEEE 802.1Q VLAN • IEEE 802.3ad Link Aggregation Control Protocol • IEEE 802.1D Spanning Tree Protocol and traffic priorities • IEEE 802.1p priority tags • IEEE 802.1w Rapid Spanning Tree Protocol • IEEE 802.1x Port Authentication • RIP (RFC 1058) • DHCP (RFC 1541) • DVMRP (RFC 1075) • ICMP (RFC 792) • IGMP (RFC 1112) • IGMPv2 (RFC 2236) • PIM-DM (draft-ietf-idmr-pim-dm-06) • RADIUS (RFC 2618) • RMON (RFC 1757 groups 1,2,3,9) • RIPv2 (RFC 2453) • OSPF (RFC 2328, 1587) • SNTP (RFC 2030) • SNMP (RFC 1157) • HTTPS • SNTP (RFC 2030) • SSH (Version 2.0)

Software Specifications (Cont.)	
Management Information Bases:	• Bridge MIB (RFC 1493) • Entity MIB (RFC 2737) • Ethernet MIB (RFC 2665) • Ether-like MIB (RFC 1643) • 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 • MIB II (RFC 1213) • PIM MIB (RFC 2934) • Port Access Entity MIB (IEEE 802.1x) • RIP1 MIB (RFC 1058) • RIP2 MIB (RFC 2453) • OSPF MIB (RFC 1850) • RADIUS Authentication Client MIB (RFC 2618) • TACACS+ Authentication Client MIB • RMON MIB (RFC 2819) • RMON II Probe Configuration Group (RFC 2021, partial implementation) • Trap (RFC 1215) • Private MIB • SNMP framework MIB (RFC 2571) • SNMP-MPD MIB (RFC 2572) • SNMP Target MIB, SNMP Notification MIB (RFC 2573) • SNMP User-Based SM MIB (RFC 2574) • SNMP View Based ACM MIB (RFC 2575) • SNMP Community MIB (RFC 2576)

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 (See *Downloading System Software from a Server* section on page 34.) The following table lists some of the basic system defaults.

System Defaults		
Function	**Parameter**	**Default**
Console Port Connection	Baud Rate	9600
	Data bits	8
	Stop bits	1
	Parity	none
	Local Console Timeout	0 (disabled)
Authentication	Privileged Exec Level	• Username "Admin" • Password "1988"
	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
	HTTPS	Enabled
	SSH	Enabled
	Port Security	Disabled
	IP Filtering	Disabled
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
	HTTP Secure Server	Enabled
	HTTP Secure Port Number	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)

System Defaults (Cont.)		
Port Configuration	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
	Port Capability	100BASE-TX/FX – • 10 Mbps half duplex • 10 Mbps full duplex • 100 Mbps half duplex • 100 Mbps full duplex • Full-duplex flow control disabled 1000BASE-T – • 10 Mbps half duplex • 10 Mbps full duplex • 100 Mbps half duplex • 100 Mbps full duplex • 1000 Mbps full duplex • Full-duplex flow control disabled • Symmetric flow control disabled 1000BASE-X – • 1000 Mbps full duplex • Full-duplex flow control disabled • Symmetric flow control disabled
Power over Ethernet	Status	Enabled (all ports)
Rate Limiting	Input and output limits	Disabled
Port Trunking	Static Trunks	None
	LACP	Disabled
Broadcast Storm Protection	Status	Enabled (all ports)
	Broadcast Limit Rate	500 packets per second
Spanning Tree Protocol	Status	Enabled, RSTP (Defaults: All values based on IEEE 802.1w)
	Fast Forwarding (Edge Port)	Disabled
Address Table	Aging Time	300 seconds
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
Traffic Prioritization	Ingress Port Priority	0
	Weighted Round Robin	• Class 0: 1 • Class 1: 4 • Class 2: 16 • Class 3: 64
	IP Precedence Priority	Enabled
	IP DSCP Priority	Disabled
	IP Port Priority	Disabled

System Defaults (Cont.)		
IP Settings	Management VLAN	1
	IP Address	0.0.0.0
	Subnet Mask	255.0.0.0
	Default Gateway	0.0.0.0
	DHCP	Enabled
	BOOTP	Disabled
	Port Security	Learning is enabled
Multicast Filtering	IGMP Snooping (Layer 2)	• Snooping: Enabled • Querier: Disabled
System Log	Status	Enabled
	Messages Logged	Levels 0-7 (all)
	Messages Logged to Flash	Levels 0-3
SNTP	Clock Synchronization	Disabled

Additional Documentation

For detailed installation, refer to the *NXA-ENET24 Hardware Installation Guide* available on-line at www.amx.com.

Initial Configuration

Connecting to the Switch

Configuration Options

This 24-Port Fast Ethernet PoE Switch switch includes a built-in network management agent. The agent offers a variety of management options, including SNMP, RMON 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

The IP address for this switch is assigned via DHCP by default. To change this address, see Setting an IP Address section on page 13.

The switch's HTTP Web agent allows you to configure switch parameters, monitor port connections, and display statistics graphically using a standard Web browser such as Netscape Navigator version 6.2 and higher or Microsoft IE version 5.0 and higher. 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 connection over the network.

The switch's management agent is based on SNMP (Simple Network Management Protocol) versions 1, 2 and 3. This SNMP agent permits the switch to be managed from any system in the network using management software.

The switch's CLI configuration program, Web interface, and SNMP agent allow you to perform the following management functions:

- Set user names and passwords
- Control port access through IEEE 802.1x security or static address filtering
- Set an IP interface for a management VLAN
- Configure SNMP parameters
- Enable/disable any port
- Set the speed/duplex mode for any port
- Power attached devices using IEEE 802.3af Power over Ethernet (PoE)
- Configure the bandwidth of any port by rate limiting
- Configure up to 255 IEEE 802.1Q VLANs
- Enable GVRP automatic VLAN registration
- Configure IGMP multicast filtering
- Upload and download system firmware via TFTP
- Upload and download switch configuration files via TFTP
- Configure Spanning Tree parameters
- Configure Class of Service (CoS) priority queuing
- Configure up to six static or LACP trunks
- Filter packets using Access Control Lists (ACLs)
- Enable port mirroring
- Set broadcast storm control on any port
- 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.

NOTE

When switches are stacked together, you must connect to the RS-232 port on the Master unit to be able to access the CLI.

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 Hardware Configuration 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's 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 data rate to 9600 baud.
   - 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

1. *When using HyperTerminal with Microsoft® Windows® 2000, make sure that you have Windows 2000 Service Pack 2 or later installed. Windows 2000 Service Pack 2 fixes the problem of arrow keys not functioning in HyperTerminal's VT100 emulation. See www.microsoft.com for information on Windows 2000 service packs.*
2. *Refer to Line Commands section on page 9 for a complete description of console configuration options.*
3. *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* section on page 171. For a list of all the CLI commands and detailed information on using the CLI, refer to *Command Groups* section on page 164.

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, DHCP or BOOTP protocol.

The IP address for this switch is assigned via DHCP by default. To manually configure this address or enable dynamic address assignment via DHCP or BOOTP, see the *Setting an IP Address* section on page 13.

NOTE

This switch supports four concurrent Telnet sessions.

After configuring the switch's IP parameters, you can access the onboard configuration program from anywhere within the attached network. The onboard configuration program 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, or Netscape Navigator 6.2 or above), or from a network computer using 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 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 *Username* prompt, enter “**admin**” (case-sensitive).
3. At the *Password* prompt, enter “**1988**” (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

Passwords can consist of up to 8 alphanumeric characters and are case sensitive. To prevent unauthorized access to the switch, set the passwords as follows:

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.

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 Intelligent Fast Ethernet PoE Switch 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)#
```

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 sends IP configuration requests to BOOTP or DHCP address allocation servers on the network.

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.

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 assigned 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
- Default gateway for the network
- Network mask for this network

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

1. From the Privileged Exec level 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
Console(config)#
```

Dynamic Configuration

If you select the "**bootp**" or "**dhcp**" option, IP will be enabled but will not function until a BOOTP or DHCP reply has been received. You therefore need to use the "ip dhcp restart" command to start broadcasting service requests.

- Requests will be sent periodically in an effort to obtain IP configuration information. (BOOTP and DHCP values can include the IP address, subnet mask, and default gateway.)
- If the "bootp" or "dhcp" option is saved to the startup-config file, 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 Privileged Exec level 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 through DHCP, type "**ip address dhcp**" and press <Enter>.
   - To obtain IP settings through BOOTP, type "**ip address bootp**" and press <Enter>.
3. Type "**exit**" to return to the global configuration mode. Press <Enter>.
4. Type "**ip dhcp restart**" to begin broadcasting service requests. Press <Enter>.

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

6. 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)#exit
Console#ip dhcp restart
Console#show ip interface
IP interface vlan
 IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 1,
 and address mode: User specified.
Console#copy running-config startup-config
Startup configuration file name []: startup

Console#
```

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 (1) respond to SNMP requests or (2) 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.

Community Strings

Community strings are used to control management access to SNMP 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 or user groups, and set the access level.

The default strings are:

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

NOTE

If you do not intend to utilize SNMP, it is recommended that you delete both of the default community strings. If there are no community strings, then SNMP management access to the switch is disabled.

To prevent unauthorized access to the switch via SNMP, 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>.

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

Trap Receivers

You can also specify SNMP stations that are to receive traps from the switch.

To configure a trap receiver, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type "**snmp-server host *host-address community-string***", where "host-address" is the IP address for the trap receiver and "community-string" is the string associated with that host. Press <Enter>.
2. In order to configure the switch to send SNMP notifications, you must enter at least one snmp-server enable traps command. Type "**snmp-server enable traps *type***", where "type" is either authentication or link-up-down. Press <Enter>.

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

Saving 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.

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.

Console#
```

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 three types of files are:

- **Configuration**: These files store system configuration information and are created when configuration settings are saved. Saved configuration files can be selected as a system start-up file or can be uploaded via TFTP to a server for backup. A file named "Factory_Default_Config.cfg" contains all the system default settings and cannot be deleted from the system. See the *Saving Configuration Settings* section on page 16 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, Web and SNMP management interfaces. See the *Managing Firmware* section on page 31 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, and two diagnostic code files. However, you can have as many configuration files as available flash memory space allows.

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.

Configuring Power over Ethernet

The 24-Port Fast Ethernet PoE Switch’s 24 10/100 Mbps ports support the IEEE 802.3af Power-over-Ethernet (PoE) standard that enables DC power to be supplied to attached devices over the unused pairs of wires in the connecting Ethernet cable.

Any 802.3af compliant device attached to a port can directly draw power from the switch over the Ethernet cable without requiring its own separate power source. This capability gives network administrators centralized power control for devices such as IP phones and wireless access points, which translates into greater network availability.

A maximum PoE power budget for the switch (power available to all switch ports) can be defined so that power can be centrally managed, preventing overload conditions at the power source. If the power demand from devices connected to the switch exceeds the power budget setting, the switch uses port power priority settings to limit the supplied power.

In the example below, the **power mainpower maximum allocation** CLI command is used to set the PoE power budget for the switch. (Range: 37 - 375 watts).

If devices connected to the switch require more power than the switch budget, the port power priority settings are used to control the supplied power. See the *Setting a Switch Power Budget* section on page 106 for details.

```
Console(config)#power mainpower maximum allocation 200
```

PoE is enabled for all ports by default.

Power can be disabled for a port by using the **no** form of the **power inline** CLI command, as shown in the example below.

```
Console(config)#interface ethernet 1/2
Console(config-if)#no power inline
Console(config-if)#
```

DHCP Relay

Since DHCP uses a broadcast mechanism, a DHCP server and its client must physically reside on the same subnet. Since it is not practical to have a DHCP server on every subnet, DHCP Relay is also supported to allow dynamic configuration of network interface blades on data network subnets/VLANs from a DHCP server located in the management network.

Web Interface

Overview

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, or Netscape Navigator 6.2 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 Chapter 4: "Command Line 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 the *Setting an IP Address* section on page 13).
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 the *Configuring User Accounts* section on page 55.)
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.
- 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.
- 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 the *Configuring Interface Settings* section on page 120.

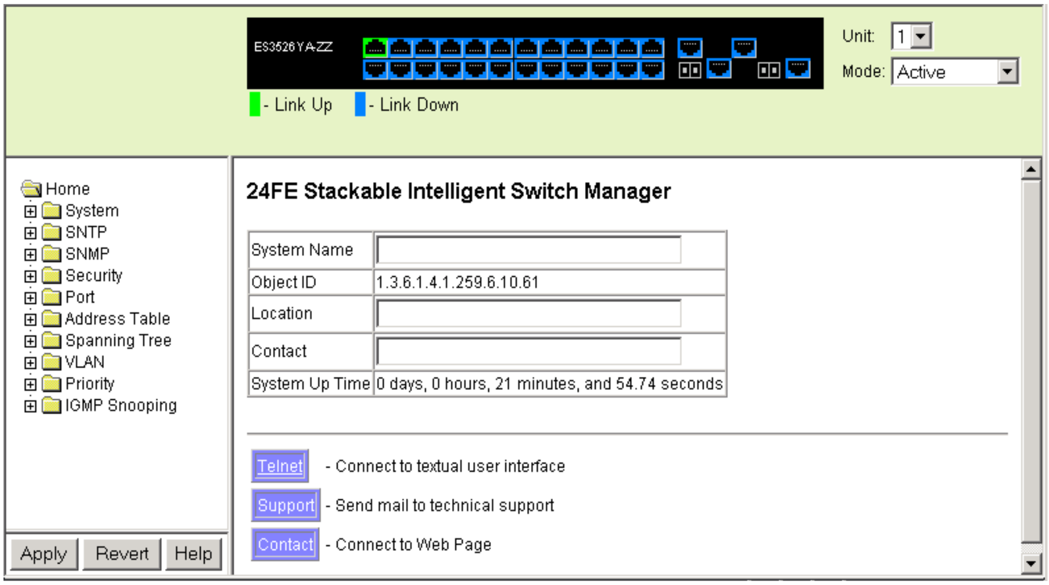
Navigating the Web Browser Interface

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**" and **1988** respectively.

Home Page

When your Web browser connects with the switch's Web agent, the home page is displayed as shown in FIG. 1. 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.



Unit: 1

Mode: Active

24FE Stackable Intelligent Switch Manager

System Name	
Object ID	1.3.6.1.4.1.259.6.10.61
Location	
Contact	
System Up Time	0 days, 0 hours, 21 minutes, and 54.74 seconds

Telnet - Connect to textual user interface

Support - Send mail to technical support

Contact - Connect to Web Page

FIG. 1 Homepage

NOTE

The examples in this chapter are based on the ES3526YA. Other than the number of fixed ports, there are no major differences between the ES3526YA and ES3550YA.

Configuration Options

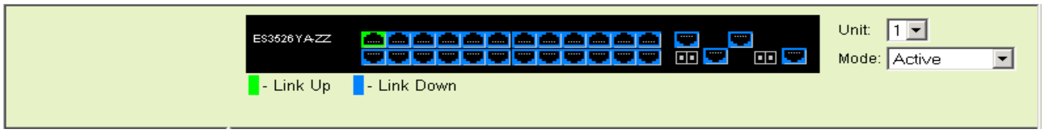
Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the **Apply** button to confirm the new setting. The following table summarizes the Web page configuration buttons.

Configuration Options	
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.

- To ensure proper screen refresh, be sure that Internet Explorer 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 pag**e."
- When using Internet Explorer, 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 (FIG. 2). 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). Clicking on the image of a port opens the *Port Configuration* page (see the *Port Configuration* section on page 85).



🟩 - Link Up 🟦 - Link Down

Unit: 1

Mode: Active

FIG. 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.

Switch Main Menu	
Menu	**Description**
System	
• System Information	Provides basic system description, including contact information
• Switch Information	Shows the number of ports, hardware/firmware version numbers, and power status
• Bridge Extension	Shows the bridge extension parameters
• IP Configuration	Sets the IP address for management access
• File	
• Copy	Enables the transfer and copying files
• Delete	Enables the deletion of files from flash memory
• Set Startup	Sets the startup files
Line	
• Console	Sets console port connection parameters
• Telnet	Sets Telnet connection parameters
Log	
• Logs	Stores and displays error messages
• System Logs	Sends error messages to a logging process
• Remote Logs	Configures the logging of messages to a remote logging process
• SMTP	Sends an SMTP client message to a participating server
• Reset	Restarts the switch
SNTP	
• SNTP Configuration	Configures SNTP client settings, including broadcast mode or a specified list of servers
• Clock Time Zone	Sets the local time zone for the system clock
SNMP	
• Configuration	Configures community strings and related trap functions
• Agent Status	Allows SNMP to be enabled or disabled
• SNMPv3	
• Engine ID	Sets the SNMP v3 engine ID
• Users	Configures SNMP v3 users
• Groups	Configures SNMP v3 groups
• Views	Configures SNMP v3 views

Switch Main Menu (Cont.)	
Menu	**Description**
Security	
• User Accounts	Configures user names and passwords
• Authentication Settings	Configures authentication sequence, RADIUS and TACACS
• HTTPS Settings	Configures secure HTTP settings
• SSH	
• Settings	Configures Secure Shell server settings
• Host-Key Settings	Generates the host key pair (public and private)
• Port Security	Configures per port security, including status, response for security breach, and maximum allowed MAC addresses
• 802.1x	Port authentication
• Information	Displays the global configuration setting
• Configuration	Configures the global configuration setting
• Port Configuration	Sets parameters for individual ports
• Statistics	Displays protocol statistics for the selected port
• ACL	
• Configuration	Configures packet filtering based on IP or MAC addresses
• Mask Configuration	Controls the order in which ACL rules are checked
• Port Binding	Binds a port to the specified ACL
• IP Filter	Sets IP addresses of clients allowed management access via the Web, SNMP, and Telnet
Port	
• Port Information	Displays port connection status
• Trunk Information	Displays trunk connection status
• Port Configuration	Configures port connection settings
• Trunk Configuration	Configures trunk connection settings
• Trunk Membership	Specifies ports to group into static trunks
• LACP	
• Configuration	Allows ports to dynamically join trunks
• Aggregation Port	Configures system priority, admin key, and port priority
• Port Counters Information	Displays statistics for LACP protocol messages
• Port Internal Information	Displays settings and operational state for local side
• Port Neighbors Information	Displays settings and operational state for remote side
• Broadcast Control	Sets the broadcast storm threshold for each port
• Mirror Port Configuration	Sets the source and target ports for mirroring
• Rate Limit	
• Input Port Configuration	Sets the input rate limit for each port
• Input Trunk Configuration	Sets the input rate limit for each trunk
• Output Port Configuration	Sets the output rate limit for each port
• Output Trunk Configuration	Sets the output rate limit for each trunk
• Port Statistics	Lists Ethernet and RMON port statistics

Switch Main Menu (Cont.)	
Menu	**Description**
PoE	
• Power Status	Displays the status of global power parameters
• Power Config	Configures the power budget for the switch
• Power Port Status	Displays the status of port power parameters
• Power Port Config	Configures port power parameters
Address Table	
• Static Addresses	Displays entries for interface, address or VLAN
• Dynamic Addresses	Displays or edits static entries in the Address Table
• Address Aging	Sets timeout for dynamically learned entries
Spanning Tree	
• STA	
• Information	Displays STA values used for the bridge
• Configuration	Configures global bridge settings for STA
• Port Information	Displays individual port settings for STA
• Trunk Information	Displays individual trunk settings for STA
• Port Configuration	Configures individual port settings for STA
• Trunk Configuration	Configures individual trunk settings for STA
VLAN	
• 802.1Q VLAN	
• GVRP Status	Enables GVRP VLAN registration protocol
• Basic Information	Displays basic information on the VLAN type supported by this switch
• Current Table	Shows the current port members of each VLAN and whether or not the port supports VLAN tagging
• Static List	Used to create or remove VLAN groups
• Static Table	Modifies the settings for an existing VLAN
• Static Membership by Port	Configures membership type for interfaces, including tagged, untagged or forbidden
• Port Configuration	Specifies default PVID and VLAN attributes
• Trunk Configuration	Specifies default trunk VID and VLAN attributes
Private VLAN	
• Private VLAN Information	Displays Private VLAN feature information
• Private VLAN Configuration	This page is used to create/remove primary or community VLANs
• Private VLAN Association	Each community VLAN must be associated with a primary VLAN
• Private VLAN Port/Trunk Information	Displays the interfaces associated with private VLANs
• Private VLAN Port/Trunk Configuration	Sets the private VLAN interface type, and associates the interfaces with a private VLAN

Switch Main Menu (Cont.)	
Menu	**Description**
Priority	
• Default Port Priority	Sets the default priority for each port
• Default Trunk Priority	Sets the default priority for each trunk
• Traffic Classes	Maps IEEE 802.1p priority tags to output queues
• Traffic Classes Status	Enables/disables traffic class priorities (not implemented)
• Queue Mode	Sets queue mode to strict priority or Weighted Round-Robin
• Queue Scheduling	Configures Weighted Round Robin queueing
• IP Precedence/DSCP Priority Status	Globally selects IP Precedence or DSCP Priority, or disables both
• IP Precedence Priority	Sets IP Type of Service priority, mapping the precedence tag to a class-of-service value
• IP DSCP Priority	Sets IP Differentiated Services Code Point priority, mapping a DSCP tag to a class-of-service value
• IP Port Priority Status	Globally enables or disables IP Port Priority
• IP Port Priority	Sets TCP/UDP port priority, defining the socket number and associated class-of-service value
• Copy Settings	Enables mapping IP Precedence and DSCP Priority settings to ports, or trunks.
• ACL CoS Priority	Sets the CoS value and corresponding output queue for packets matching an ACL rule
• ACL Marker	Change traffic priorities for frames matching an ACL rule
IGMP Snooping	
• IGMP Configuration	Enables multicast filtering; configures parameters for multicast query
• Multicast Router Port Information	Displays the ports that are attached to a neighboring multicast router/switch for each VLAN ID
• Static Multicast Router Port Configuration	Assigns ports that are attached to a neighboring multicast router/switch
• IP Multicast Registration Table	Displays all multicast groups active on this switch, including multicast IP addresses and VLAN ID
• IGMP Member Port Table	Indicates multicast addresses associated with the selected VLAN
DNS	
• General Configuration	Enables DNS; configures domain name and domain list; and specifies IP address of name servers for dynamic lookup
• Static Host Table	Configures static entries for domain name to address mapping
• Cache	Displays cache entries discovered by designated name servers

Basic Configuration

Displaying System Information

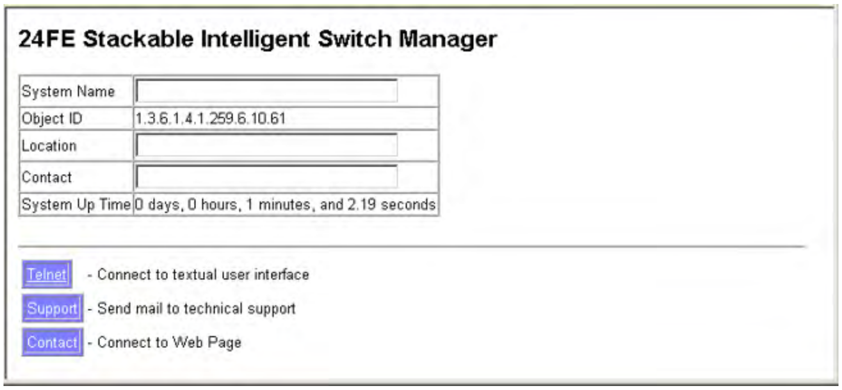
You can easily identify the system by providing a descriptive name, location and contact information.

Field Attributes	
• **Model Number:**	The switch model number.
• **S/W Version #:**	The current software version number.
• **System Name:**	Name assigned to the switch system.
• **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.
These additional parameters are displayed for the CLI.	
• **MAC Address:**	The physical layer address for this switch.
• **Web server:**	Shows if management access via HTTP is enabled.
• **Web server port:**	Shows the TCP port number used by the web interface.
• **Web secure server:**	Shows if management access via HTTPS is enabled.
• **Web secure server port:**	Shows the TCP port used by the HTTPS interface.
• **Telnet server:**	Shows if management access via Telnet is enabled.
• **Telnet server port:**	Shows the TCP port number used by Telnet.
• **Authentication login:**	Defines the login authentication method and precedence.
• **Authentication enable:**	Defines the authentication method and precedence to use when changing from Exec command mode to Privileged Exec command mode
• **POST result:**	Shows results of the power-on self-test.

Displaying System Information - Web

Click *System*, *System Information*. Specify the system name, location, and contact information for the system administrator, then click **Apply**.

This page also includes a Telnet button that access the Command Line Interface via Telnet (FIG. 3).



24FE Stackable Intelligent Switch Manager

System Name	
Object ID	1.3.6.1.4.1.259.6.10.61
Location	
Contact	
System Up Time	0 days, 0 hours, 1 minutes, and 2.19 seconds

Telnet - Connect to textual user interface

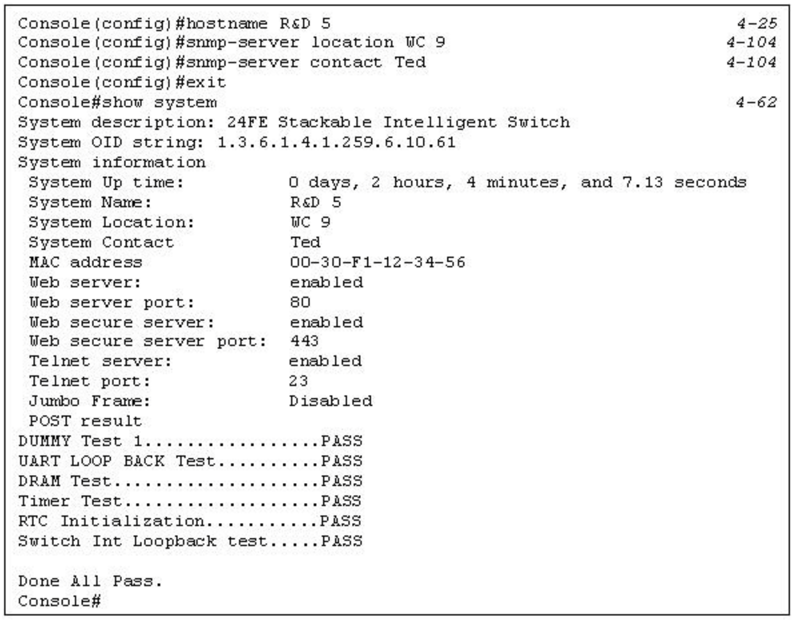
Support - Send mail to technical support

Contact - Connect to Web Page

FIG. 3 Web - Displaying System Information

Displaying System Information - CLI

Specify the hostname, location and contact information.



```
Console(config)#hostname R&D 5                                      4-25
Console(config)#snmp-server location WC 9                          4-104
Console(config)#snmp-server contact Ted                            4-104
Console(config)#exit
Console#show system                                                 4-62
System description: 24FE Stackable Intelligent Switch
System OID string: 1.3.6.1.4.1.259.6.10.61
System information
 System Up time:          0 days, 2 hours, 4 minutes, and 7.13 seconds
 System Name:             R&D 5
 System Location:         WC 9
 System Contact           Ted
 MAC address              00-30-F1-12-34-56
 Web server:              enabled
 Web server port:         80
 Web secure server:       enabled
 Web secure server port:  443
 Telnet server:           enabled
 Telnet port:             23
 Jumbo Frame:             Disabled
 POST result
DUMMY Test 1.................PASS
UART LOOP BACK Test..........PASS
DRAM Test....................PASS
Timer Test...................PASS
RTC Initialization...........PASS
Switch Int Loopback test.....PASS

Done All Pass.
Console#
```

FIG. 4 CLI - Displaying System Information

Displaying Switch Hardware/Software Versions

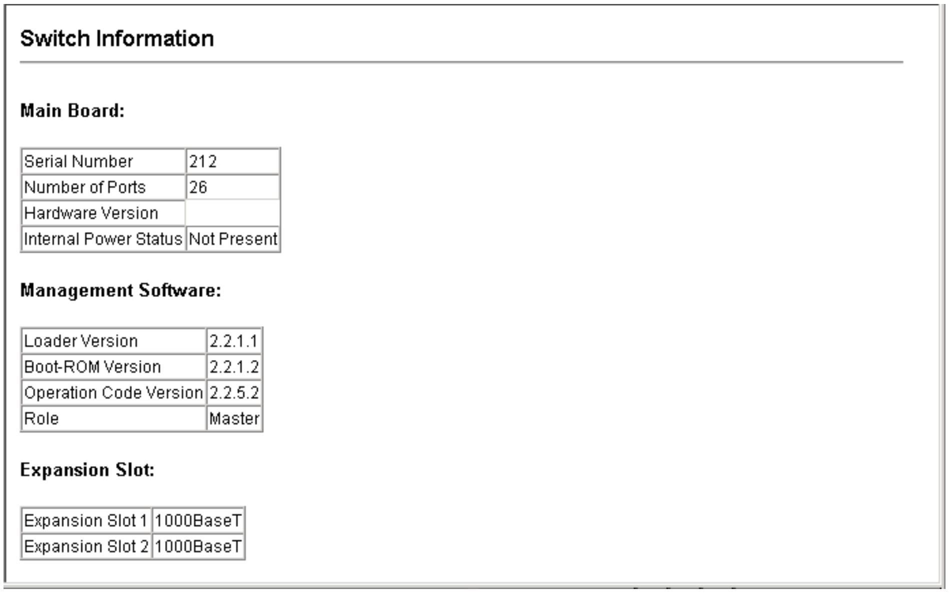
Use the Switch Information page to display hardware/firmware version numbers for the main board and management software, as well as the power status of the system.

Field Attributes

Field Attributes	
Main Board	
• **Serial Number:**	The serial number of the switch.
• **Number of Ports:**	Number of built-in RJ-45 ports and expansion ports.
• **Hardware Version:**	Hardware version of the main board.
• **Internal Power Status:**	Displays the status of the internal power supply.
• **Redundant Power Status:**	Displays the status of the redundant power supply. CLI only
Management Software	
• **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 (i.e., operating stand-alone).
Expansion Slot	
• **Expansion Slot 1/2**	Slots for extender transceivers.
These additional parameters are displayed for the CLI:	
• **Unit ID:**	Unit number in stack.
• **Redundant Power Status:**	Displays the status of the redundant power supply.

Displaying Switch Hardware/Software Versions - Web

Click *System, Switch Information*.



Switch Information

Main Board:

Serial Number	212
Number of Ports	26
Hardware Version	
Internal Power Status	Not Present

Management Software:

Loader Version	2.2.1.1
Boot-ROM Version	2.2.1.2
Operation Code Version	2.2.5.2
Role	Master

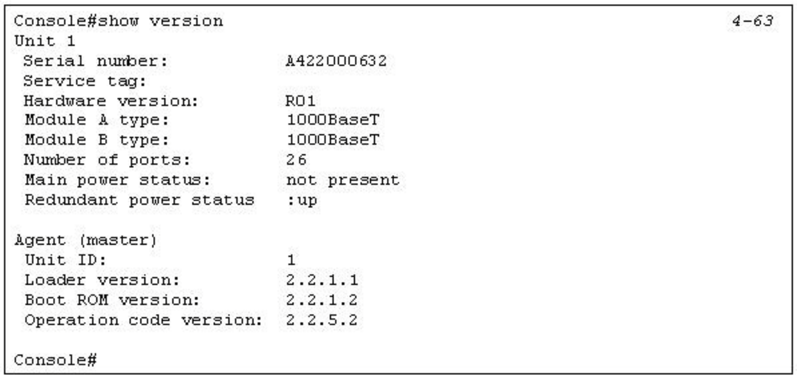
Expansion Slot:

Expansion Slot 1	1000BaseT
Expansion Slot 2	1000BaseT

FIG. 5 CLI - Display Switch Information

Displaying Switch Hardware/Software Versions - CLI

Use the **Console#show version** command to display version information.



```
Console#show version                                                4-63
Unit 1
 Serial number:              A422000632
 Service tag:
 Hardware version:           R01
 Module A type:              1000BaseT
 Module B type:              1000BaseT
 Number of ports:            26
 Main power status:          not present
 Redundant power status      :up

Agent (master)
 Unit ID:                    1
 Loader version:             2.2.1.1
 Boot ROM version:           2.2.1.2
 Operation code version:     2.2.5.2

Console#
```

FIG. 6 Web - Displaying Switch Information

Displaying Bridge Extension Capabilities

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, or to configure the global setting for GARP VLAN Registration Protocol (GVRP).

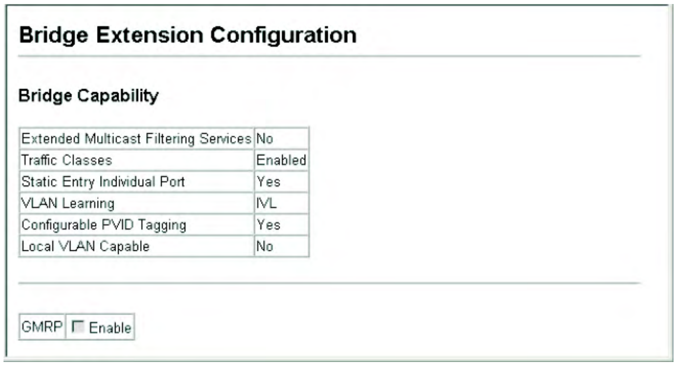
Field Attributes

Field Attributes	
• **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 the *Class of Service Configuration* section on page 137.)
• **Static Entry Individual Port:**	This switch allows static filtering for unicast and multicast addresses. (Refer to the *Setting Static Addresses* section on page 109.)
• **VLAN Learning:**	This switch uses Independent VLAN Learning (IVL), where each port maintains its own filtering database.

Field Attributes (Cont.)	
• **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 the *VLAN Configuration* section on page 123.
• **Local VLAN Capable:**	This switch does not support multiple local bridges (i.e., multiple Spanning Trees).
• **GMRP:**	GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups. This switch does not support GMRP; it uses the Internet Group Management Protocol (IGMP) to provide automatic multicast filtering.

Displaying Bridge Extension Capabilities - Web

Click *System, Bridge Extension*.



Bridge Extension Configuration

Bridge Capability

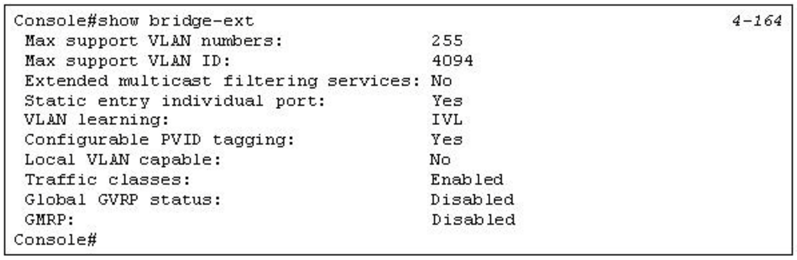
Extended Multicast Filtering Services	No
Traffic Classes	Enabled
Static Entry Individual Port	Yes
VLAN Learning	IVL
Configurable PVID Tagging	Yes
Local VLAN Capable	No

GMRP ☐ Enable

FIG. 7 Web - Displaying Bridge Extension Configuration

Displaying Bridge Extension Capabilities - CLI

Enter the **Console#show bridge-ext** command (FIG. 8).



```
Console#show bridge-ext                                                    4-164
 Max support VLAN numbers:                 255
 Max support 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#
```

FIG. 8 CLI - Displaying Bridge Extension Configuration

Setting the IP Address

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

To manually configure an address, you need to change the switch's default settings (IP address 0.0.0.0 and netmask 255.0.0.0) 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 (if routing is not enabled on this switch).

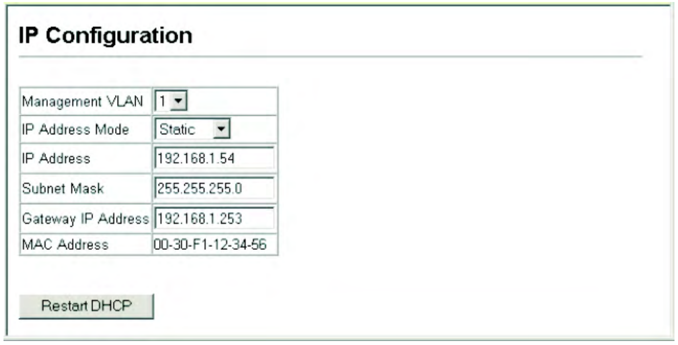
You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.

Command Attributes

Command Attributes	
• **Management VLAN:**	This is the only VLAN through which you can gain management access to the switch. By default, all ports on the switch are members of VLAN 1, so a management station can be connected to any port on the switch. However, if other VLANs are configured and you change the Management VLAN, you may lose management access to the switch. In this case, you should reconnect the management station to a port that is a member of the Management VLAN.
• **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 values can include the IP address, subnet mask, and default gateway.)
• **IP Address:**	Address of the VLAN interface that is allowed management access. Valid IP addresses consist of four numbers, 0 to 255, separated by periods.
• **Subnet Mask:**	This mask identifies the host address bits used for routing to specific subnets.
• **Gateway IP Address:**	IP address of the gateway router between this device and management stations that exist on other network segments.
• **MAC Address:**	The MAC address of this switch.
• **Restart DHCP:**	Releases the current IP address and requests a new IP address from the DHCP server.

Manual Configuration - Web

Click *System*, *IP*. Specify the management interface, IP address and default gateway, then click **Apply**.



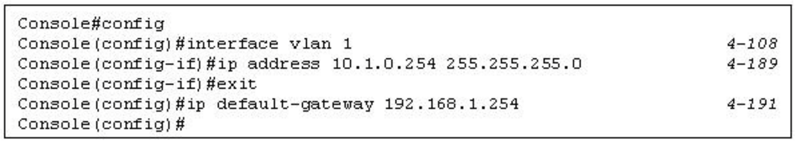
IP Configuration

Management VLAN	1
IP Address Mode	Static
IP Address	192.168.1.54
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.253
MAC Address	00-30-F1-12-34-56

FIG. 9 Web - Manual Web IP Configuration

Manual Configuration - CLI

Specify the management interface, IP address and default gateway:



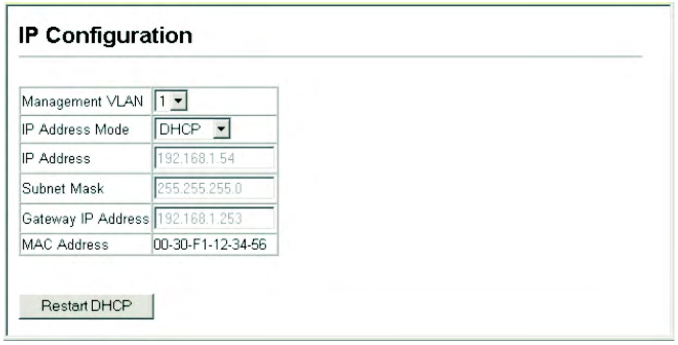
```
Console#config
Console(config)#interface vlan 1                                    4-108
Console(config-if)#ip address 10.1.0.254 255.255.255.0              4-189
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254                    4-191
Console(config)#
```

FIG. 10 CLI - Manual Web IP Configuration

Using DHCP/BOOTP - Web

If your network provides DHCP/BOOTP services, you can configure the switch to be dynamically configured by these services. Click *System*, *IP*. Specify the Management VLAN, set the IP Address Mode to *DHCP* or *BOOTP*, and click **Apply** to save your changes.

The switch will broadcast a request for IP configuration settings on the next power reset. Otherwise, you can click **Restart DHCP** to immediately request a new address.



IP Configuration

Management VLAN	1
IP Address Mode	DHCP
IP Address	192.168.1.54
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.253
MAC Address	00-30-F1-12-34-56

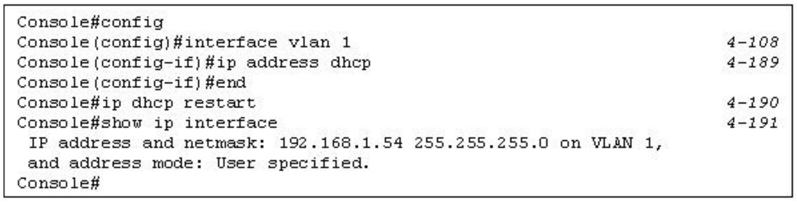
FIG. 11 Web - IP Configuration using DHCP

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

NOTE

Using DHCP/BOOTP - CLI

Specify the management interface, and set the IP address mode to *DHCP* or *BOOTP*, and then enter the "**ip dhcp restart**" command:



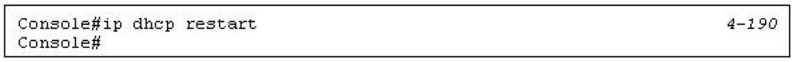
```
Console#config
Console(config)#interface vlan 1                                    4-108
Console(config-if)#ip address dhcp                                  4-189
Console(config-if)#end
Console#ip dhcp restart                                             4-190
Console#show ip interface                                           4-191
 IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
 and address mode: User specified.
Console#
```

FIG. 12 CLI - IP Configuration using DHCP

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.

- **Web** – 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.
- **CLI** – Enter the **Console#ip dhcp restart** command to restart DHCP service:



```
Console#ip dhcp restart                                             4-190
Console#
```

FIG. 13 CLI - Renewing DHCP

Managing Firmware

You can upload/download firmware to or from a TFTP server. By saving runtime code to a file on a TFTP server, that file can later be downloaded to the switch to restore operation. You can set the switch to use new firmware without overwriting the previous version.

The switch also allows a runtime code file to be copied to or from another switch unit in the stack.

Command Attributes

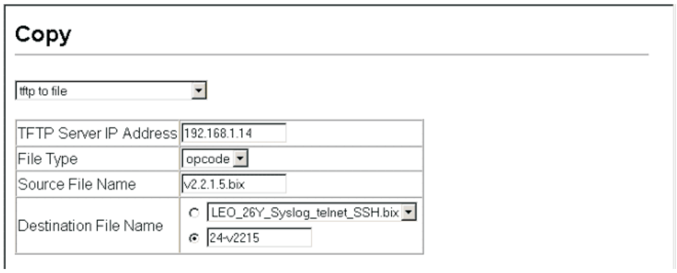
Command Attributes	
• **File Transfer Method:**	The firmware copy operation includes these options: • file to file - Copies a file within the switch directory, assigning it a new name. • file to tftp - Copies a file from the switch to a TFTP server. • ftp to file - Copies a file from a TFTP server to the switch. • file to unit - Copies a file from this switch to another unit in the stack. • unit to file - Copies a file from another unit in the stack to this switch.
• **TFTP Server IP Address:**	The IP address of a TFTP server.
• **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 on the TFTP server is 127 characters or 31 characters for files on the switch. Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”
• **Source/Destination Unit:**	Specifies the switch stack unit number.
• **File Type:**	Allows you to specify either an operational code file (opcode), or a configuration file (config).

Up to two copies of the system software (i.e., the runtime firmware) can be stored in the file directory on the switch. The currently designated startup version of this file cannot be deleted.

Downloading System Software from a Server - Web

When downloading runtime code, you can specify the Destination File Name to replace the current image, or first download the file using a different name from the current runtime code file, and then set the new file as the startup file.

Click *System*, *File*, *Copy*. Select “**tftp to file**” from the drop-down menu. Select “**opcode**” as the file type, then enter the IP address of the TFTP server and the source and destination file names. Click **Apply**.



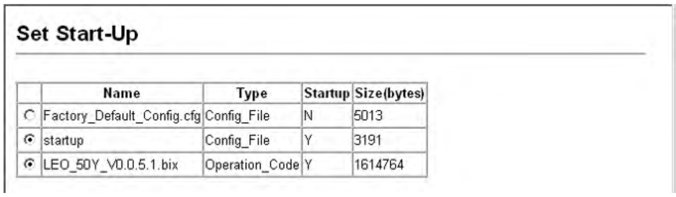
Copy

tftp to file

TFTP Server IP Address	192.168.1.14
File Type	opcode
Source File Name	v2.2.1.5.bix
Destination File Name	○ LEO_26Y_Syslog_telnet_SSH.bix ● 24-v2215

FIG. 14 Operation Code Image File Transfer

If you download to a new destination file, select the file from the drop-down box for the operation code used at startup, and click **Apply**. To start the new firmware, reboot the system via the System/Reset menu.



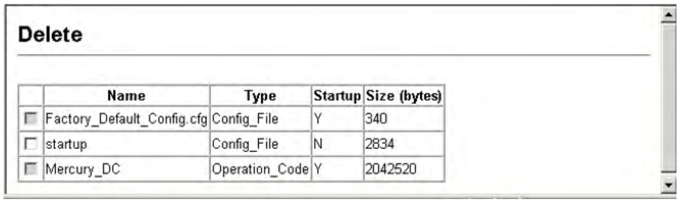
Set Start-Up

	Name	Type	Startup	Size(bytes)
○	Factory_Default_Config.cfg	Config_File	N	5013
●	startup	Config_File	Y	3191
●	LEO_50Y_V0.0.5.1.bix	Operation_Code	Y	1614764

FIG. 15 Select Start-Up Operation File

To delete a file, select *System*, *File*, *Delete*. Select the file name from the given list by checking the tick box and then click **Apply**.

Note that the file currently designated as the startup code cannot be deleted.



Delete

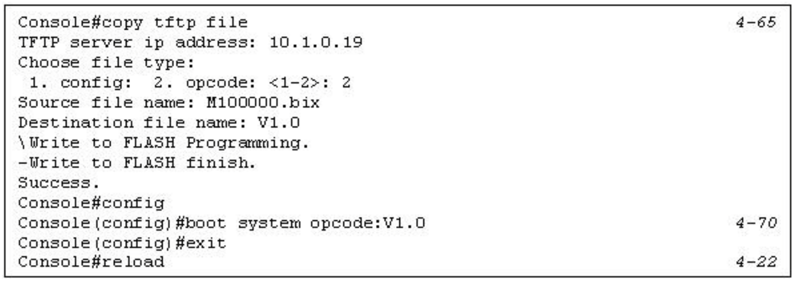
	Name	Type	Startup	Size (bytes)
□	Factory_Default_Config.cfg	Config_File	Y	340
□	startup	Config_File	N	2834
□	Mercury_DC	Operation_Code	Y	2042520

FIG. 16 Deleting Files

Downloading System Software from a Server - CLI

To download new firmware form a TFTP server, enter the IP address of the TFTP server, select “**opcode**” as the file type, then enter the source and destination file names. When the file has completed the download, set the new file to start up the system and then restart the switch.

To start the new firmware, enter the “**reload**” command or reboot the system (FIG. 17).



```
Console#copy tftp file                                              4-65
TFTP server ip address: 10.1.0.19
Choose file type:
 1. config:  2. opcode: <1-2>: 2
Source file name: M100000.bix
Destination file name: V1.0
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#config
Console(config)#boot system opcode:V1.0                             4-70
Console(config)#exit
Console#reload                                                      4-22
```

FIG. 17 CLI - Downloading System Software from a Server

Saving or Restoring Configuration Settings

You can upload/download configuration setting files to/from a TFTP server or copy files to and from switch units in a stack. The configuration files can be later downloaded to restore the switch's settings.

Command Usage

- When updating the PoE controller, first copy the PD controller file from a TFTP server to the switch's file system (tftp to file), and then copy this file to the controller (file to file).
- When specifying the file type "P**D_Controller**" or "**PoE**" for copy operations via the web or CLI, file types other than PoE controller may be downloaded, but will not adversely affect the system.

Command Attributes

Command Attributes	
• **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 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. • running-config to file - Copies the running configuration to a file. • 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 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. • file to unit - Copies a file from this switch to another unit in the stack. • unit to file - Copies a file from another unit in the stack to this switch.
• **TFTP Server IP Address:**	The IP address of a TFTP server.
• **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 on the TFTP server is 127 characters or 31 characters for files on the switch. Valid characters: A-Z, a-z, 0-9, ".", "-", "_"
• **Source/Destination Unit:**	Specifies the switch stack unit number.
• **File Type:**	Allows you to specify an operational code (opcode), a configuration (config), or a PoE controller (PD_Controller) file.

NOTE

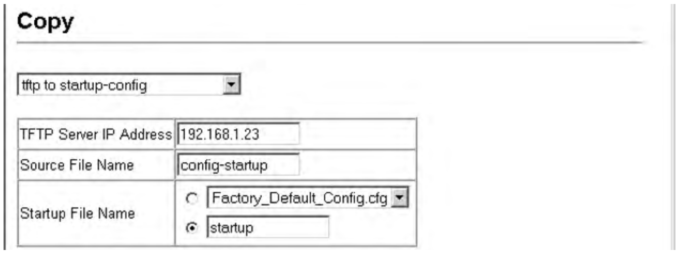
The maximum number of user-defined configuration files is limited only by available flash memory space.

Downloading Configuration Settings from a Server - Web

You can download the configuration file under a new file name and then set it as the startup file, or you can specify the current startup configuration file as the destination file to directly replace it. Note that the file "**Factory_Default_Config.cfg**" can be copied to the TFTP server, but cannot be used as the destination on the switch.

Click *System*, *File*, *Copy*. Select "**tftp to startup-config**" or "**tftp to file**" and enter the IP address of the TFTP server.

Specify the name of the file to download and select a file on the switch to overwrite or specify a new file name, then click **Apply**.



Copy

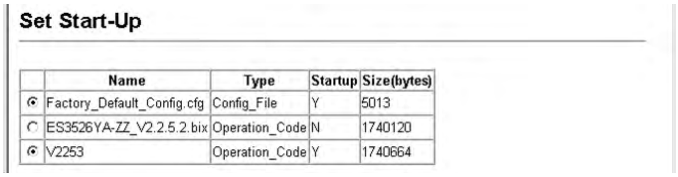
tftp to startup-config

TFTP Server IP Address	192.168.1.23
Source File Name	config-startup
Startup File Name	○ Factory_Default_Config.cfg ● startup

FIG. 18 Copy Configuration Settings

If you download to a new file name using "**tftp to startup-config**" or "**tftp to file**", the file is automatically set as the start-up configuration file. To use the new settings, reboot the system via the System/Reset menu.

Note that you can also select any configuration file as the start-up configuration by using the *System/File/Set Start-Up* page.



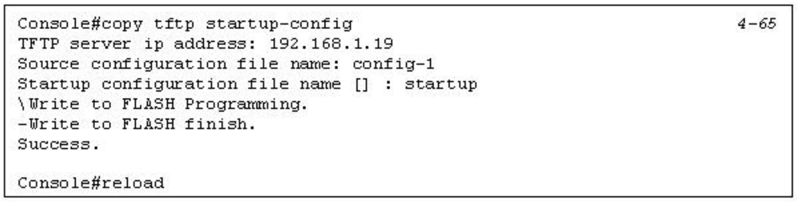
Set Start-Up

	Name	Type	Startup	Size(bytes)
●	Factory_Default_Config.cfg	Config_File	Y	5013
○	ES3526YA-ZZ_V2.2.5.2.bix	Operation_Code	N	1740120
●	V2253	Operation_Code	Y	1740664

FIG. 19 Setting the Startup Configuration Settings

Downloading Configuration Settings from a Server - CLI

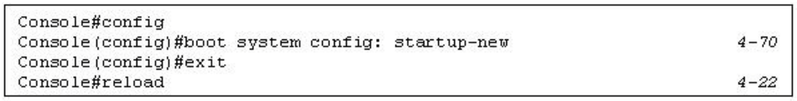
Enter the IP address of the TFTP server, specify the source file on the server, set the startup file name on the switch, and then restart the switch (FIG. 20).



```
Console#copy tftp startup-config                                     4-65
TFTP server ip address: 192.168.1.19
Source configuration file name: config-1
Startup configuration file name [] : startup
\Write to FLASH Programming.
-Write to FLASH finish.
Success.

Console#reload
```

FIG. 20 CLI - Downloading Configuration Settings from a Server

To select another configuration file as the start-up configuration, use the **boot system** command and then restart the switch (FIG. 21).



```
Console#config
Console(config)#boot system config: startup-new                      4-70
Console(config)#exit
Console#reload                                                       4-22
```

FIG. 21 CLI - Boot System

This example shows how to download a PoE controller file from a TFTP server.

```
Console#copy tftp file                                                  233
TFTP server IP address: 10.3.4.50
Choose file type:
 1. config: 2. opcode 3. PD_Controller: <1-3>: 3
Source file name: 7012_007.s19
Destination file name: PoE-test
Write to FLASH Programming.
Write to FLASH finish.
Success.
Console#
```

This example shows how to copy a PoE controller file from another unit in the stack.

```
Console#copy file controller                                           233
Unit <1-2>: 2
Choose controller type:
 1. PoE: 2. VDSL: 3. TBD <1-3>: 1
Source file name: PoE-test
Software downloading in progress, please wait...
Unit 1 done
Console#
```

Console Port Settings

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, timeouts, and basic communication settings. These parameters can be configured via the Web or CLI interface.

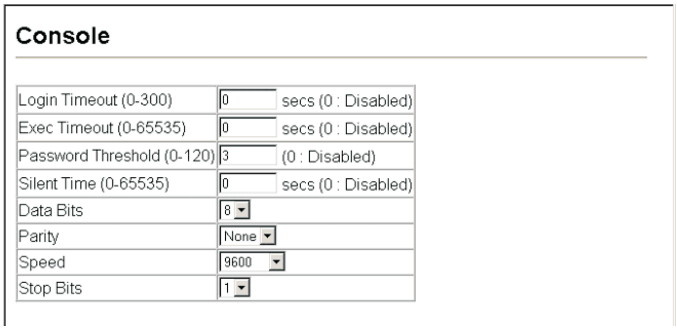
Command Attributes

Command Attributes	
• **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
• **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 • Default: 0
• **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

Command Attributes (Cont.)	
• **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 or specify "Auto." • Default: 9600 bps
• **Stop Bits:**	Sets the number of the stop bits transmitted per byte. • Default: 1 stop bit
• **Password:**	Specifies a password for the line connection. 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. • Default: No password. • CLI only.
• **Login:**	Enables password checking at login. You can select authentication by a single global password as configured for the Password parameter, or by passwords set up for specific username accounts (the default). • CLI only.

Console Port Settings - Web

Click *System*, *Line*, *Console*. Specify the console port connection parameters as required, then click **Apply**.



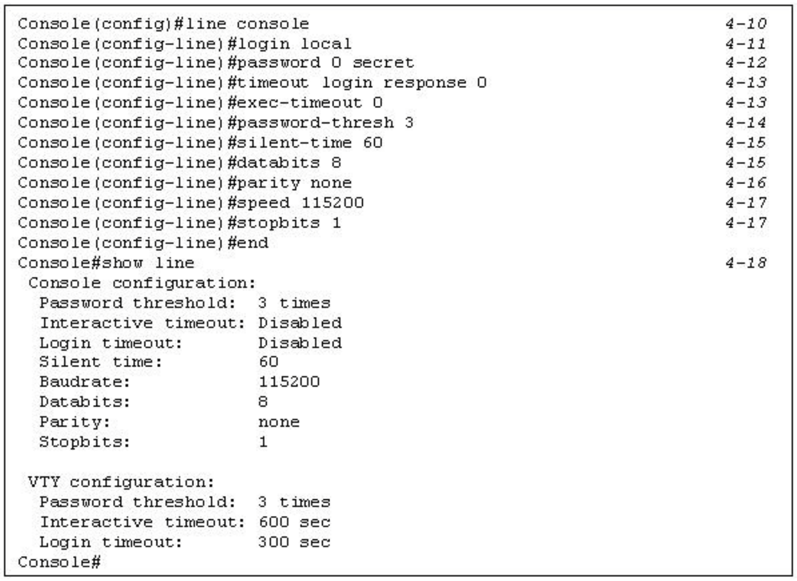
Console

Login Timeout (0-300)	0	secs (0 : Disabled)
Exec Timeout (0-65535)	0	secs (0 : Disabled)
Password Threshold (0-120)	3	(0 : Disabled)
Silent Time (0-65535)	0	secs (0 : Disabled)
Data Bits	8	
Parity	None	
Speed	9600	
Stop Bits	1	

FIG. 22 Console Port Settings

Console Port Settings - CLI

Enter Line Configuration mode for the console, then specify the connection parameters as required. To display the current console port settings, use the **show line** command from the Normal Exec level (FIG. 23).



```
Console(config)#line console                                        4-10
Console(config-line)#login local                                    4-11
Console(config-line)#password 0 secret                              4-12
Console(config-line)#timeout login response 0                       4-13
Console(config-line)#exec-timeout 0                                 4-13
Console(config-line)#password-thresh 3                              4-14
Console(config-line)#silent-time 60                                 4-15
Console(config-line)#databits 8                                     4-15
Console(config-line)#parity none                                    4-16
Console(config-line)#speed 115200                                   4-17
Console(config-line)#stopbits 1                                     4-17
Console(config-line)#end
Console#show line                                                   4-18
 Console configuration:
  Password threshold:  3 times
  Interactive timeout: Disabled
  Login timeout:       Disabled
  Silent time:         60
  Baudrate:            115200
  Databits:            8
  Parity:              none
  Stopbits:            1

 VTY configuration:
  Password threshold:  3 times
  Interactive timeout: 600 sec
  Login timeout:       300 sec
Console#
```

FIG. 23 CLI - Console Port Settings

Telnet Settings

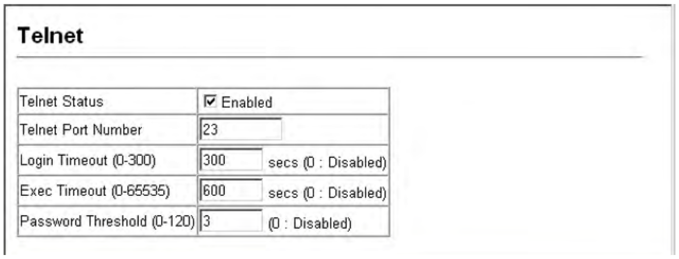
You can access the onboard configuration program over the network using Telnet (i.e., a virtual terminal). Management access via Telnet can be enabled/disabled and other various parameters set, including the TCP port number, timeouts, and a password. These parameters can be configured via the Web or CLI interface.

Command Attributes

Command Attributes	
• **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
• **Password:**	Specifies a password for the line connection. 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. • Default: No password • CLI only.
• **Login:**	Enables password checking at login. You can select authentication by a single global password as configured for the Password parameter, or by passwords set up for specific user-name accounts (the default). • CLI only.

Telnet Settings - Web

Click *System*, *Line*, *Telnet*. Specify the connection parameters for Telnet access, then click **Apply**.



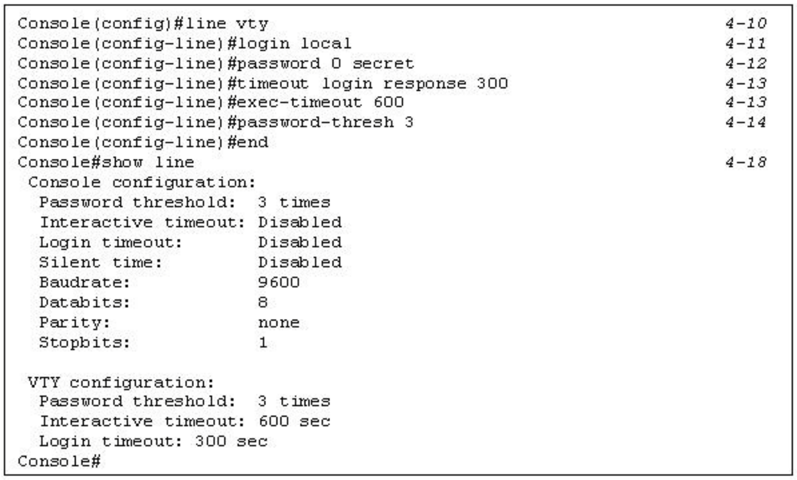
Telnet

Telnet Status	☑ Enabled	
Telnet Port Number	23	
Login Timeout (0-300)	300	secs (0 : Disabled)
Exec Timeout (0-65535)	600	secs (0 : Disabled)
Password Threshold (0-120)	3	(0 : Disabled)

FIG. 24 Web - Enabling Telnet

Telnet Settings - CLI

Enter Line Configuration mode for a virtual terminal, then specify the connection parameters as required. To display the current virtual terminal settings, use the **show line** command from the Normal Exec level.



```
Console(config)#line vty                                          4-10
Console(config-line)#login local                                  4-11
Console(config-line)#password 0 secret                            4-12
Console(config-line)#timeout login response 300                   4-13
Console(config-line)#exec-timeout 600                             4-13
Console(config-line)#password-thresh 3                            4-14
Console(config-line)#end
Console#show line                                                 4-18
 Console configuration:
  Password threshold:  3 times
  Interactive timeout: Disabled
  Login timeout:       Disabled
  Silent time:         Disabled
  Baudrate:            9600
  Databits:            8
  Parity:              none
  Stopbits:            1

 VTY configuration:
  Password threshold:  3 times
  Interactive timeout: 600 sec
  Login timeout: 300 sec
Console#
```

FIG. 25 Enabling Telnet - CLI

Configuring Event Logging

Overview

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

The system allows you 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.
- The System Logs 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.

Command Attributes

Command Attributes	
• **System Log Status:**	Enables/disables the logging of debug or error messages to the logging process.
• **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 See the Logging Levels table on page 39for details.
• **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: 6) ***Note**: The Flash Level must be equal to or less than the RAM Level.*

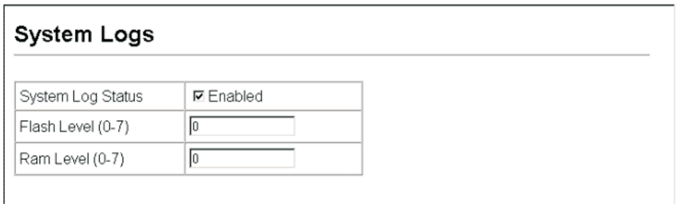
Logging Levels

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.

System Log Configuration - Web

Click *System*, *Log*, *System Logs*. Specify System Log Status, then change the level of messages to be logged to RAM and flash memory, then click **Apply**.



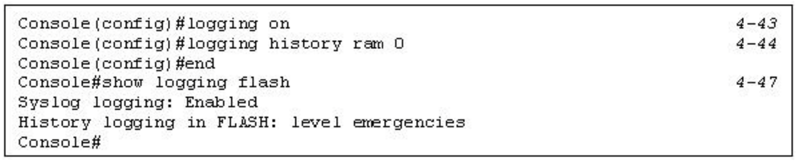
System Logs

System Log Status	☑ Enabled
Flash Level (0-7)	0
Ram Level (0-7)	0

FIG. 26 Web - System Logs

System Log Configuration - CLI

Enable system logging and then specify the level of messages to be logged to RAM and flash memory. Use the **show logging** command to display the current settings. Type "**show log ram**" to display log messages in the RAM buffer.



```
Console(config)#logging on                                          4-43
Console(config)#logging history ram 0                               4-44
Console(config)#end
Console#show logging flash                                          4-47
Syslog logging: Enabled
History logging in FLASH: level emergencies
Console#
```

FIG. 27 CLI - System Logs

Remote Logs Configuration

The *Remote Logs* page allows you to configure the logging of messages that are sent to syslog servers. You can also limit the error messages sent to only those messages below a specified level.

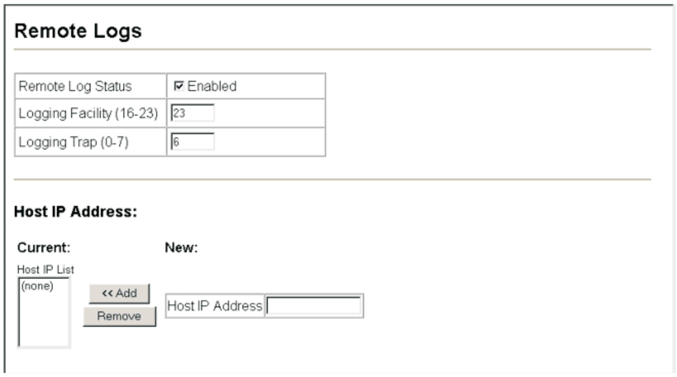
Command Attributes

Command Attributes	
• **Remote Log Status:**	Enables/disables the logging of debug or error messages to the remote logging process. • Default: Enabled
• **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. • 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. • Default: 3
• **Host IP List:**	Displays the list of remote server IP addresses that receive the syslog messages. The maximum number of host IP addresses allowed is five.
• **Host IP Address:**	Specifies a new server IP address to add to the Host IP List.

Remote Logs Configuration - Web

Click *System*, *Log*, *Remote Logs*. To add an IP address to the Host IP List, type the new IP address in the Host IP Address box, and then click **Add**.

To delete an IP address, click the entry in the Host IP List, and then click **Remove**.



Remote Logs

Remote Log Status	☑ Enabled
Logging Facility (16-23)	23
Logging Trap (0-7)	6

Host IP Address:

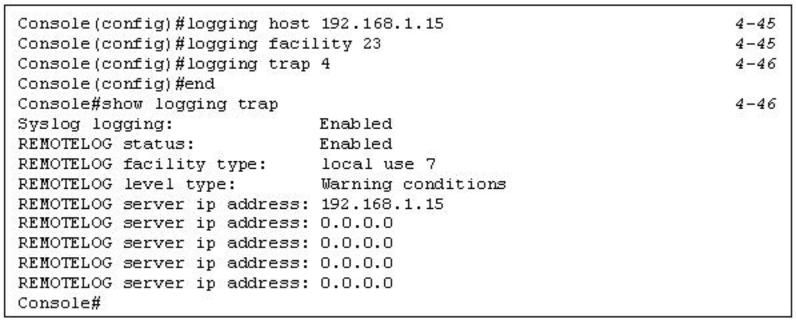
Current: Host IP List (none)

New: Host IP Address

FIG. 28 Remote Logs

Remote Logs Configuration - CLI

Enter the syslog server host IP address, choose the facility type and set the logging trap.



```
Console(config)#logging host 192.168.1.15                                 4-45
Console(config)#logging facility 23                                       4-45
Console(config)#logging trap 4                                            4-46
Console(config)#end
Console#show logging trap                                                 4-46
Syslog logging:             Enabled
REMOTELOG status:           Enabled
REMOTELOG facility type:    local use 7
REMOTELOG level type:       Warning conditions
REMOTELOG server ip address: 192.168.1.15
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#
```

FIG. 29 Remote Logs

Displaying Log Messages

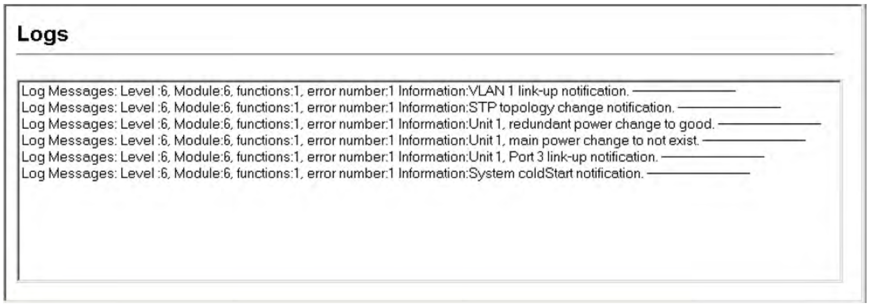
The Logs page allows you to scroll through the logged system and event messages.

NOTE

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.

Displaying Log Messages - Web

Click *System*, *Log*, *Logs*.



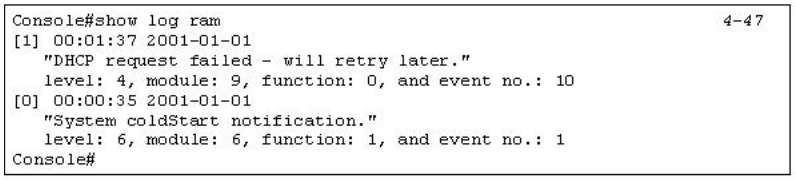
Logs

```
Log Messages: Level :6, Module:6, functions:1, error number:1 Information:VLAN 1 link-up notification.
Log Messages: Level :6, Module:6, functions:1, error number:1 Information:STP topology change notification.
Log Messages: Level :6, Module:6, functions:1, error number:1 Information:Unit 1, redundant power change to good.
Log Messages: Level :6, Module:6, functions:1, error number:1 Information:Unit 1, main power change to not exist.
Log Messages: Level :6, Module:6, functions:1, error number:1 Information:Unit 1, Port 3 link-up notification.
Log Messages: Level :6, Module:6, functions:1, error number:1 Information:System coldStart notification.
```

FIG. 30 Displaying Logs

Displaying Log Messages - CLI

This example shows the event message stored in RAM.



```
Console#show log ram                                                    4-47
[1] 00:01:37 2001-01-01
   "DHCP request failed - will retry later."
   level: 4, module: 9, function: 0, and event no.: 10
[0] 00:00:35 2001-01-01
   "System coldStart notification."
   level: 6, module: 6, function: 1, and event no.: 1
Console#
```

FIG. 31 Displaying Logs

Sending SMTP Alerts

To alert system administrators of problems, the switch can use SMTP (Simple Mail Transfer Protocol) to send 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.

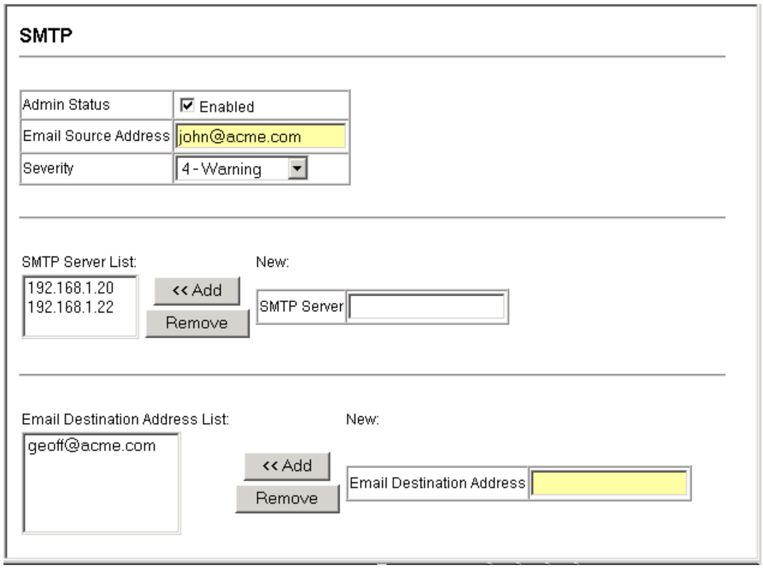
Command Attributes

Command Attributes	
• **Admin Status:**	Enables/disables the SMTP function. • Default: Disabled
• **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 used to trigger alert messages (see the *Logging Levels* section on page 39). 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. Use the *New Email Destination Address* text field and the Add/Remove buttons to configure the list.

Sending SMPT Alerts - Web

Click *System*, *Log*, *SMTP*. Enable SMTP, specify a source email address, and select the minimum severity level.

- To add an IP address to the SMTP Server List, type the new IP address in the SMTP Server text box and then click **Add**.
- To delete an IP address, click the entry in the SMTP Server List and then click **Remove**. Specify up to five email addresses to receive the alert messages, and then click **Apply**.



SMTP

Admin Status	☑ Enabled
Email Source Address	john@acme.com
Severity	4 - Warning ▾

SMTP Server List:
192.168.1.20
192.168.1.22

New: SMTP Server

Email Destination Address List:
geoff@acme.com

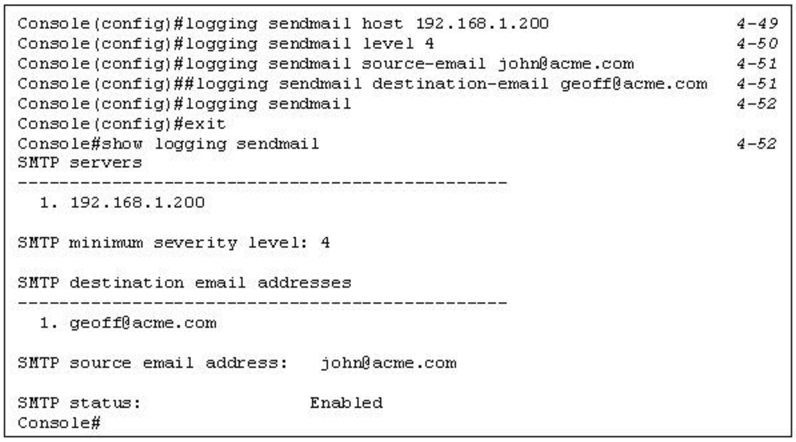
New: Email Destination Address

FIG. 32 Web - Enabling and Configuring SMTP Alerts

Sending SMPT Alerts - CLI

Enter the IP address of at least one SMTP server, set the syslog severity level to trigger an email message, and specify the switch (source) and up to five recipient (destination) email addresses. Enable SMTP with the **logging sendmail** command to complete the configuration.

Use the **show logging sendmail** command to display the current SMTP configuration.



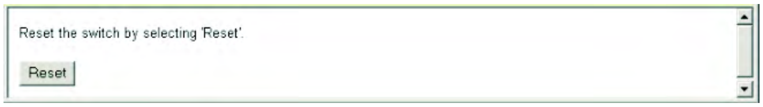
```
Console(config)#logging sendmail host 192.168.1.200                  4-49
Console(config)#logging sendmail level 4                             4-50
Console(config)#logging sendmail source-email john@acme.com          4-51
Console(config)##logging sendmail destination-email geoff@acme.com   4-51
Console(config)#logging sendmail                                     4-52
Console(config)#exit
Console#show logging sendmail                                        4-52
SMTP servers
-----------------------------------------------
  1. 192.168.1.200

SMTP minimum severity level: 4

SMTP destination email addresses
-----------------------------------------------
  1. geoff@acme.com

SMTP source email address:   john@acme.com

SMTP status:                 Enabled
Console#
```

FIG. 33 CLI - Enabling and Configuring SMTP Alerts

Resetting the System

Resetting the System - Web

Select *System*, *Reset* to reboot the switch. When prompted, confirm that you want reset the switch.



Reset the switch by selecting 'Reset'.

FIG. 34 Web - Resetting the Switch

Resetting the System - CLI

Use the **reload** command to reboot the system.

```
Console#reload                                                    4-22
System will be restarted, continue <y/n>? y
Console#
```

FIG. 35 CLI - Resetting the Switch

NOTE

When restarting the system, it always runs the Power-On Self-Test.

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 using the CLI. (See “calendar set” on page 225.) If the clock is not set, the switch will only record the time from the factory default set at the last bootup.

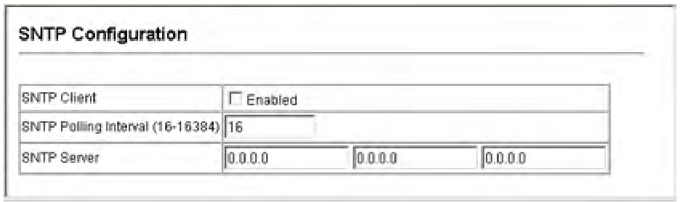
SNTP Configuration - This switch acts as an SNTP client in a unicast mode. The switch periodically sends a request for a time update to a configured time server. You can configure up to three time server IP addresses. The switch attempts to poll each server in the configured sequence.

Command Attributes

Command Attributes	
• **SNTP Client:**	Configures the switch to operate as an SNTP unicast client. This requires at least one time server to be specified in the SNTP Server field.
• **SNTP Poll Interval:**	Sets the interval between sending requests for a time update from a time server. • Range: 16-16284 seconds • Default: 16 seconds
• **SNTP Server:**	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.

Setting the System Clock - Web

Select *SNTP*, *Configuration*. Modify any of the required parameters and click **Apply**.



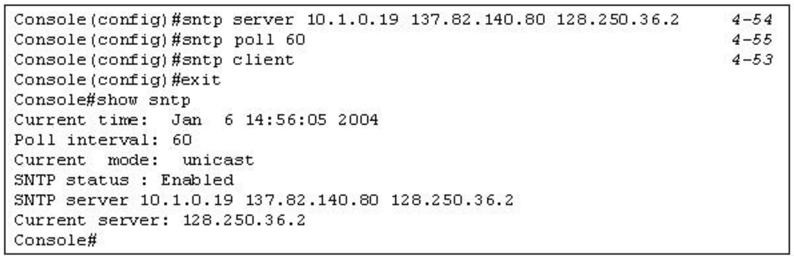
SNTP Configuration

SNTP Client	□ Enabled		
SNTP Polling Interval (16-16384)	16		
SNTP Server	0.0.0.0	0.0.0.0	0.0.0.0

FIG. 36 Web - Configuring SNTP

Setting the System Clock - CLI

This example configures the switch to operate as an SNTP unicast client and then displays the current time and settings:



```
Console(config)#sntp server 10.1.0.19 137.82.140.80 128.250.36.2      4-54
Console(config)#sntp poll 60                                          4-55
Console(config)#sntp client                                           4-53
Console(config)#exit
Console#show sntp
Current time:  Jan  6 14:56:05 2004
Poll interval: 60
Current  mode:  unicast
SNTP status : Enabled
SNTP server 10.1.0.19 137.82.140.80 128.250.36.2
Current server: 128.250.36.2
Console#
```

FIG. 37 CLI - Configuring SNTP

Setting the Time Zone

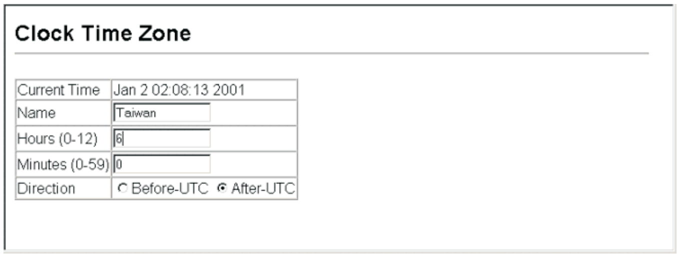
SNTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth’s prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (after) or west (before) of UTC.

Command Attributes

Command Attributes	
• **Current Time:**	Displays the current time.
• **Name:**	Assigns a name to the time zone. (Range: 1-29 characters)
• **Hours (0-12):**	The number of hours before/after UTC**.**
• **Minutes (0-59):**	The number of minutes before/after UTC.
• **Direction:**	Configures the time zone to be before (west) or after (east) UTC.

Setting the Time Zone - Web

Select *SNTP*, *Clock Time Zone*. Set the offset for your time zone relative to the UTC, and click **Apply**.



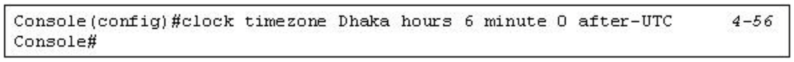
Clock Time Zone

Current Time	Jan 2 02:08:13 2001
Name	Taiwan
Hours (0-12)	6
Minutes (0-59)	0
Direction	○ Before-UTC ● After-UTC

FIG. 38 Web - Setting the System Clock

Setting the Time Zone - CLI

This example shows how to set the time zone for the system clock.



```
Console(config)#clock timezone Dhaka hours 6 minute 0 after-UTC       4-56
Console#
```

FIG. 39 CLI - Setting the System Clock

SNMP Protocol

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 software such as HP OpenView.

Access to the onboard agent 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 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.

SNMPv3 Security Models and Levels

The following table shows the security models and levels available and the system default settings.

SNMPv3 Security Models and Levels

Model	Level	Group	Read View	Write View	Security
v1	noAuthNoPriv	public (read only)	defaultview	none	Community string only
v1	noAuthNoPriv	private (read/write)	defaultview	defaultview	Community string only
v1	noAuthNoPriv	user defined	user defined	user defined	Community string only
v2c	noAuthNoPriv	public (read only)	defaultview	none	Community string only
v2c	noAuthNoPriv	private (read/write)	defaultview	defaultview	Community string only
v2c	noAuthNoPriv	user defined	user defined	user defined	Community string only
v3	noAuthNoPriv	user defined	user defined	user defined	A user name match only
v3	AuthNoPriv	user defined	user defined	user defined	Provides user authentication via MD5 or SHA algorithms
v3	AuthPriv	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.

Enabling SNMP

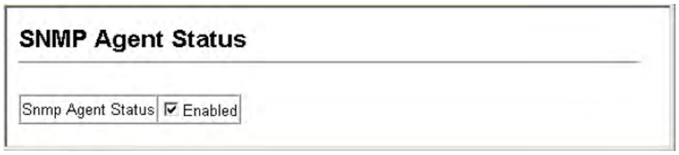
Enables SNMPv3 service for all management clients (i.e., versions 1, 2c, 3).

Command Attributes

Command Attributes	
• **SNMP Agent Status:**	Enables SNMP on the switch.

Enabling SNMP - Web

Select *SNMP, Agent Status*.



SNMP Agent Status

Snmp Agent Status ☑ Enabled

FIG. 40 Web - Enabling the SNMP Agent

Enabling SNMP - CLI

The following example enables SNMP on the switch.

```
Console(config)#snmp-server                                          293
Console(config)#
```

Setting Community Access Strings

You may configure up to five community strings authorized for management access using SNMP v1 and v2c. All community strings used for IP Trap Managers should be listed in this table.

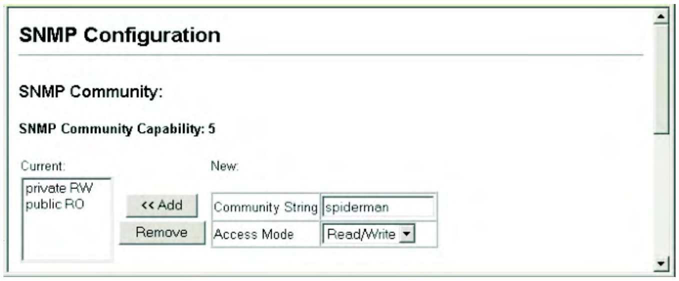
For security reasons, you should consider removing the default strings.

Command Attributes

Command Attributes	
• **SNMP Community Capability:**	Indicates that the switch supports up to five community strings.
• **Current:**	Displays a list of the community strings currently configured.
• **Community String:**	A community string that acts like a password and permits access to the SNMP protocol. • Default strings: “public” (read-only access), “private” (read/write access) • Range: 1-32 characters, case sensitive
• **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.

Setting Community Access Strings - Web

Click SNMP, SNMP Configuration. Add new community strings as required, select the access rights from the Access Mode drop-down list, then click **Add**.



SNMP Configuration

SNMP Community:

SNMP Community Capability: 5

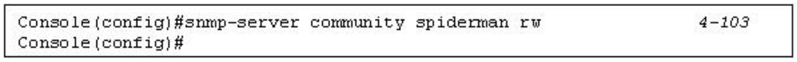
Current:
private RW
public RO

New:
Community String: spiderman
Access Mode: Read/Write

FIG. 41 Web - Configuring SNMP Community Strings

Setting Community Access Strings - CLI

The following example adds the string “spiderman” with read/write access.



```
Console(config)#snmp-server community spiderman rw              4-103
Console(config)#
```

FIG. 42 CLI - Configuring SNMP Community Strings

Specifying Trap Managers and Trap Types

Traps indicating status changes are issued by the switch to specified trap managers. You must specify trap managers so that key events are reported by this switch to your management station (using network management platforms such as HP OpenView). You can specify up to five management stations that will receive authentication failure messages and other trap messages from the switch.

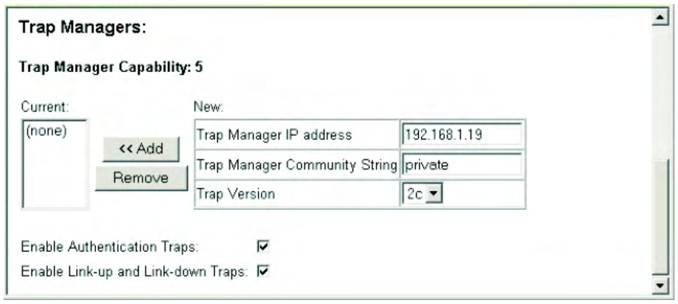
Command Attributes

Command Attributes	
• **Trap Manager Capability:**	Indicates that the switch supports up to five trap managers.
• **Current:**	Displays a list of the trap managers currently configured.
• **Trap Manager IP Address:**	IP address of a new management station to receive trap messages.
• **Trap Manager Community String:**	Specifies a valid community string for the new trap manager entry. Though you can set this string in the Trap Managers table, we recommend that you define this string in the SNMP Protocol table as well. • Range: 1-32 characters, case sensitive
• **Trap UDP Port:**	Specifies the UDP port number used by the trap manager.
• **Trap Version:**	Indicates if the user is running SNMP v1, v2c, or v3.
• **Enable Authentication Traps:**	Issues a trap message to specified IP trap managers whenever authentication of an SNMP request fails. (Default: Enabled)
• **Enable Link-up and Link-down Traps:**	Issues a trap message whenever a port link is established or broken. • Default: Enabled

Specifying Trap Managers and Trap Types - Web

Click *SNMP*, *Configuration*. Enter the IP address and community string for each management station that will receive trap messages, specify the UDP port and SNMP version, and then click **Add**.

Select the trap types required using the check boxes for Authentication and Link-up/down traps, and then click **Apply**.



Trap Managers:

Trap Manager Capability: 5

Current:

(none)

New:

Trap Manager IP address	192.168.1.19
Trap Manager Community String	private
Trap Version	2c

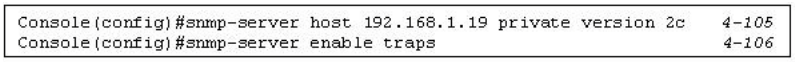
Enable Authentication Traps: ☑

Enable Link-up and Link-down Traps: ☑

FIG. 43 Web - Configuring IP Trap Managers

Specifying Trap Managers and Trap Types - CLI

This example adds a trap manager and enables authentication traps.



```
Console(config)#snmp-server host 192.168.1.19 private version 2c    4-105
Console(config)#snmp-server enable traps                            4-106
```

FIG. 44 CLI - Configuring IP Trap Managers

Configuring SNMPv3 Management Access

To configure SNMPv3 management access to the switch, follow these steps:

1. If you want to change the default engine ID, it must be changed first before configuring other parameters.
2. Specify read and write access views for the switch MIB tree.
3. Configure SNMP user groups with the required security model (i.e., SNMP v1, v2c or v3) and security level (i.e., authentication and privacy).
4. Assign SNMP users to groups, along with their specific authentication and privacy passwords.

Setting an Engine ID

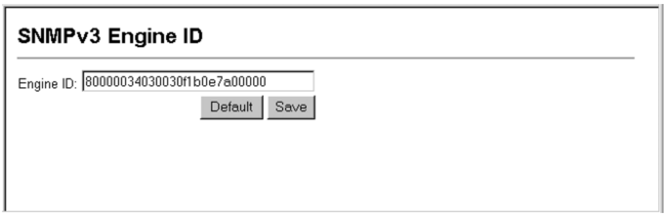
An SNMPv3 engine is an independent SNMP agent that resides on the switch. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.

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.

A new engine ID can be specified by entering 1 to 26 hexadecimal characters. If less than 26 characters are specified, trailing zeroes are added to the value. For example, the value “1234” is equivalent to “1234” followed by 22 zeroes.

Setting an Engine ID - Web

Click SNMP, SNMPv3, Engine ID. Enter an ID of up to 26 hexadecimal characters and then click **Save**.



SNMPv3 Engine ID

Engine ID: 80000034030030f1b0e7a00000

FIG. 45 Setting an Engine ID

Setting an Engine ID - CLI

This example sets an SNMPv3 engine ID.

```
Console(config)#snmp-server engine-id local 12345abcdef
Console(config)#exit
Console#show snmp engine-id294
Local SNMP engineID: 12345abcdef000000000000000
Local SNMP engineBoots: 1
Console#
```

Configuring SNMPv3 Users

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 and a write view.

Command Attributes

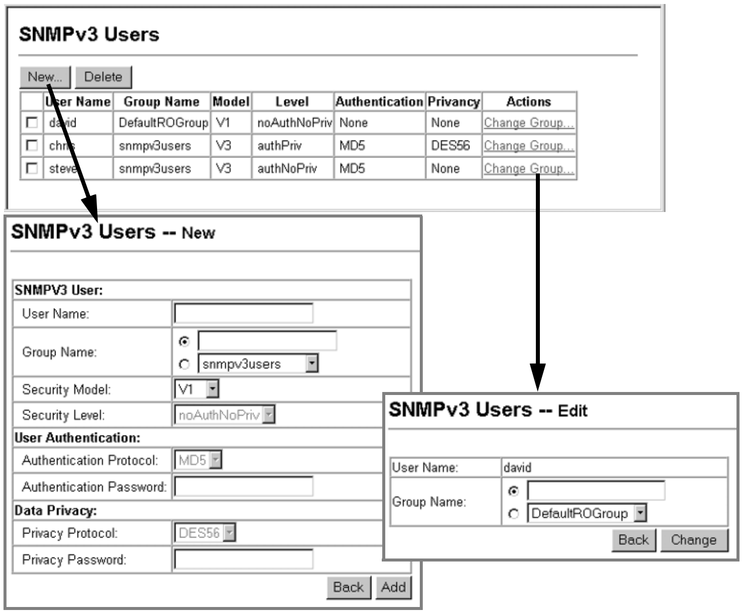
Command Attributes	
• **User Name:**	The name of user connecting to the SNMP agent. (Range: 1-32 characters)
• **Group Name:**	The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
• **Model:**	The user security model; SNMP v1, v2c or v3.
• **Level:**	The security level used for the user: • **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications. • **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model). • **AuthPriv** – SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).

Command Attributes (Cont.)	
• **Authentication:**	The method used for user authentication; MD5 or SHA
• **Privacy:**	The encryption algorithm use for data privacy; only 56-bit DES is currently available
• **Actions:**	Enables the user to be assigned to another SNMPv3 group.

Configuring SNMPv3 Users - Web

Click *SNMP*, *SNMPv3*, *Users*. Click **New** to configure a user name. In the New User page, define a name and assign it to a group, then click **Add** to save the configuration and return to the User Name list.

- To delete a user, check the box next to the user name, then click **Delete**.
- To change the assigned group of a user, click **Change Group** in the *Actions* column of the users table and select the new group.



SNMPv3 Users

	User Name	Group Name	Model	Level	Authentication	Privancy	Actions
□	david	DefaultROGroup	V1	noAuthNoPriv	None	None	Change Group...
□	chris	snmpv3users	V3	authPriv	MD5	DES56	Change Group...
□	steve	snmpv3users	V3	authNoPriv	MD5	None	Change Group...

SNMPv3 Users -- New

SNMPV3 User:	
User Name:	
Group Name:	● ○ snmpv3users
Security Model:	V1
Security Level:	noAuthNoPriv
User Authentication:	
Authentication Protocol:	MD5
Authentication Password:	
Data Privacy:	
Privacy Protocol:	DES56
Privacy Password:	

SNMPv3 Users -- Edit

User Name:	david
Group Name:	● ○ DefaultROGroup

FIG. 46 Configuring SNMPv3 Users

Configuring SNMPv3 Users - CLI

Use the **snmp-server user** command to configure a new user name and assign it to a group.

```
Console(config)#snmp-server user chris group r&d v3 auth md5 greenpeace priv des56 einstien

Console(config)#exit
Console#show snmp user299
EngineId: 80000034030001f488f5200000
User Name: chris
Authentication Protocol: md5
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

Console#
```

Configuring SNMPv3 Groups

An SNMPv3 group sets the access policy for its assigned users, restricting them to specific read and write views. You can use the pre-defined default groups or create new groups to map a set of SNMP users to SNMP views.

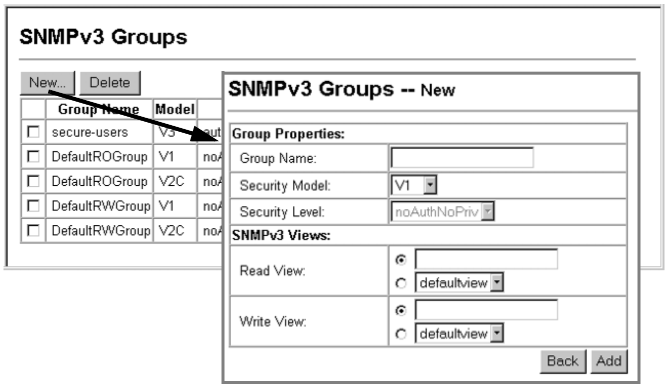
Command Attributes

Command Attributes	
• **Group Name:**	The name of the SNMP group. (Range: 1-32 characters)
• **Model:**	The group security model; SNMP v1, v2c or v3.
• **Level:**	The security level used for the group: • **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications. • **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model). • **AuthPriv** – SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).
• **Read View:**	The configured view for read access. (Range: 1-64 characters)
• **Write View:**	The configured view for write access. (Range: 1-64 characters)

Configuring SNMPv3 Groups - Web

Click *SNMP*, *SNMPv3*, *Groups*. Click **New** to configure a new group. In the *New Group* page, define a name, assign a security model and level, and then select read and write views.

- Click **Add** to save the new group and return to the Groups list.
- To delete a group, check the box next to the group name, then click **Delete**.



SNMPv3 Groups

New... Delete

	Group Name	Model	
□	secure-users	V3	aut
□	DefaultROGroup	V1	noA
□	DefaultROGroup	V2C	noA
□	DefaultRWGroup	V1	noA
□	DefaultRWGroup	V2C	noA

SNMPv3 Groups -- New

Group Properties:

Group Name:

Security Model: V1

Security Level: noAuthNoPriv

SNMPv3 Views:

Read View: ● ○ defaultview

Write View: ● ○ defaultview

Back Add

FIG. 47 Configuring SNMPv3 Groups

Configuring SNMPv3 Groups - CLI

Use the **snmp-server group** command to configure a new group, specifying the security model and level, and restricting MIB access to defined read and write views.

```
Console(config)#snmp-server group v3secure v3 priv read defaultview write defaultview 296
Console(config)#exit
Console#show snmp group297
Group Name: v3secure
Security Model: v3
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: nonvolatile
Row Status: active

Console#
```

Setting SNMPv3 Views

SNMPv3 views are used to restrict user access to specified portions of the MIB tree. The predefined view "defaultview" includes access to the entire MIB tree.

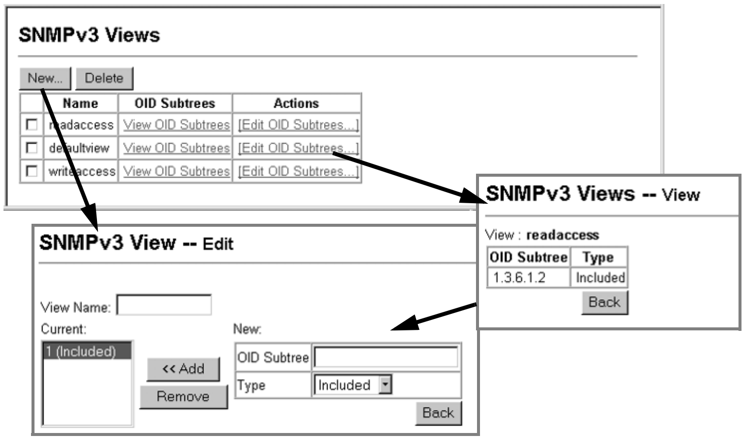
Command Attributes

Command Attributes	
• **View Name:**	The name of the SNMP view. (Range: 1-64 characters)
• **View OID Subtrees:**	Shows the currently configured object identifiers of branches within the MIB tree that define the SNMP view.
• **Edit OID Subtrees:**	Allows you to configure the object identifiers of branches within the MIB tree. Wildcards can be used to mask a specific portion of the OID string.
• **Type:**	Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view.

Setting SNMPv3 Views - Web

Click *SNMP*, *SNMPv3*, *Views*. Click **New** to configure a new view. In the *New View* page, define a name and specify OID subtrees in the switch MIB to be included or excluded in the view.

- Click **Back** to save the new view and return to the SNMPv3 Views list.
- For a specific view, click on **View OID Subtrees** to display the current configuration, or click on Edit OID Subtrees to make changes to the view settings.
- To delete a view, check the box next to the view name, then click **Delete**.



SNMPv3 Views

	Name	OID Subtrees	Actions
□	readaccess	View OID Subtrees	[Edit OID Subtrees...]
□	defaultview	View OID Subtrees	[Edit OID Subtrees...]
□	writeaccess	View OID Subtrees	[Edit OID Subtrees...]

SNMPv3 Views -- View

View : **readaccess**

OID Subtree	Type
1.3.6.1.2	Included

SNMPv3 View -- Edit

View Name:

Current: 1 (Included)

New:

OID Subtree:

Type: Included

FIG. 48 Web - Configuring SNMPv3 Views

Setting SNMPv3 Views - CLI

Use the **snmp-server view** command to configure a new view.

This example view includes the MIB-2 interfaces table, and the wildcard mask selects all index entries.

```
Console(config)#snmp-server view ifEntry.a 1.3.6.1.2.1.2.2.1.1.* included                295
Console(config)#exit
Console#show snmp view296
View Name: ifEntry.a
Subtree OID: 1.3.6.1.2.1.2.2.1.1.*
View Type: included
Storage Type: nonvolatile
Row Status: active

View Name: readaccess
Subtree OID: 1.3.6.1.2
View Type: included
Storage Type: nonvolatile
Row Status: active

View Name: defaultview
Subtree OID: 1
View Type: included
Storage Type: nonvolatile
Row Status: active

Console#
```

User Authentication

Overview

You can restrict management access to this switch and provide secure network 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.
- **HTTPS Settings** – Provide a secure web connection.
- **SSH Settings** – Provide a secure shell (for secure Telnet access).
- **Port Security** – Configure secure addresses for individual ports.
- **802.1x** – Use IEEE 802.1x port authentication to control access to specific ports.

Configuring User Accounts

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.

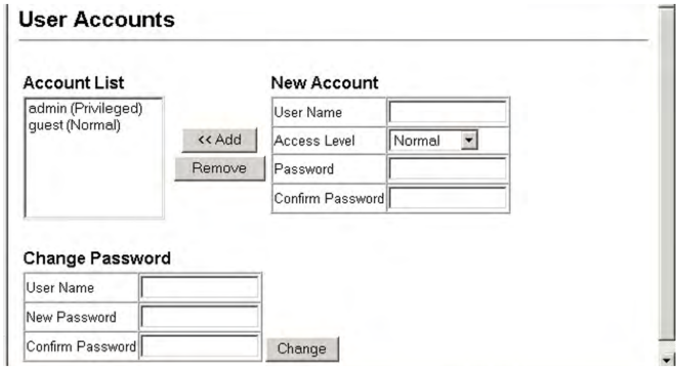
- The default guest name is “**guest**” with the password “**guest**.”
- The default administrator name is “**admin**” with the password “**admin**.”

Command Attributes

Command Attributes	
• **Account List:**	Displays the current list of user accounts and associated access levels. • Defaults: admin and guest
• **New Account:**	Allows configuration of a new account with Normal or Privileged access.
• **Add/Remove:**	Adds or removes an account from the list.
• **User Name:**	The name of the user. Maximum length: 8 characters)
• **Access Level:**	Specifies the user level. • Options: Normal and Privileged
• **Password:**	Specifies the user password. • Range: 0-8 characters plain text • case sensitive
• **Change Password:**	Sets a new password to overwrite an old password for the specified user name.

Configuring User Accounts - Web

Click *Security*, *User Accounts*. To configure a new user account, specify a user name, select the user’s access level, then enter a password and confirm it. Click **Add** to save the new user account and add it to the Account List. To change the password for a specific user, enter the user name and new password, confirm the password by entering it again, then click **Apply**.



User Accounts

Account List

admin (Privileged)
guest (Normal)

New Account

User Name	
Access Level	Normal
Password	
Confirm Password	

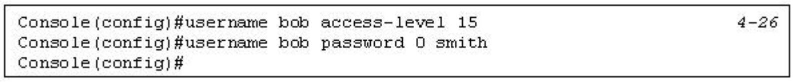
Change Password

User Name	
New Password	
Confirm Password	

FIG. 49 Web - Access Levels

Configuring User Accounts - CLI

Assign a user name to **access-level 15** (i.e., administrator), then specify the password.

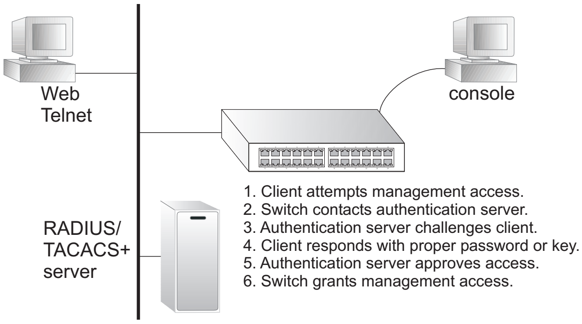


```
Console(config)#username bob access-level 15                         4-26
Console(config)#username bob password 0 smith
Console(config)#
```

FIG. 50 CLI - Access Levels

Configuring Local/Remote Logon Authentication

Use the *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.



1. Client attempts management access.
2. Switch contacts authentication server.
3. Authentication server challenges client.
4. Client responds with proper password or key.
5. Authentication server approves access.
6. Switch grants management access.

FIG. 51 Local/Remote Logon Authentication

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.

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.
- 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.

Command Attributes

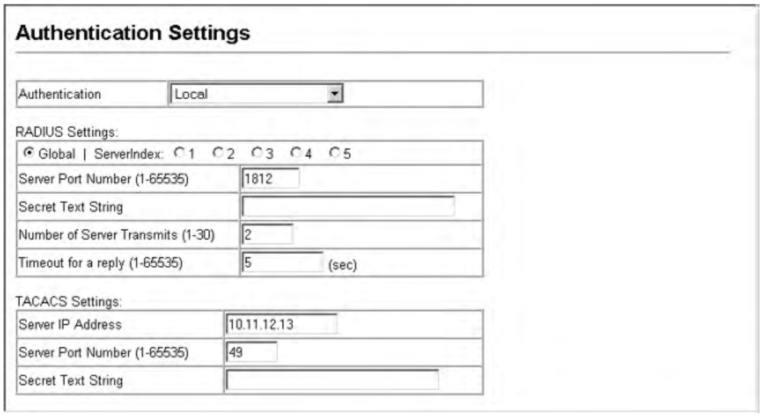
Command Attributes	
• **Authentication:**	Select the authentication, or authentication sequence required: • Local – User authentication is performed only locally by the switch. • Radius – User authentication is performed using a RADIUS server only. • TACACS – User authentication is performed using a 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. (Default: 10.1.0.1) • Server Port Number – Network (UDP) port of authentication server used for authentication messages. Range: 1-65535 Default: 1812 • Secret Text String – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. Maximum length: 20 characters • Number of Server Transmits – Number of times the switch tries to authenticate logon access via the authentication server. Range: 0-2147483647 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: 0-2147483647 Default: 5
• **TACACS Settings:**	• Server IP Address – Address of the TACACS+ server. Default: 10.11.12.13 • Server Port Number – Network (TCP) port of TACACS+ server used for authentication messages. Range: 1-65535 Default: 49 • Secret Text String – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. Maximum length: 20 characters

NOTE

The local switch user database has to be set up by manually entering user names and passwords using the CLI. (See "username" on page 196.)

Authentication Settings - Web

Click *Security*, *Authentication Settings*. To configure local or remote authentication preferences, specify the authentication sequence (i.e., one to three methods), fill in the parameters for RADIUS or TACACS+ authentication if selected, and click **Apply**.



Authentication Settings

Authentication	Local

RADIUS Settings:

● Global | ServerIndex: ○1 ○2 ○3 ○4 ○5	
Server Port Number (1-65535)	1812
Secret Text String	
Number of Server Transmits (1-30)	2
Timeout for a reply (1-65535)	5 (sec)

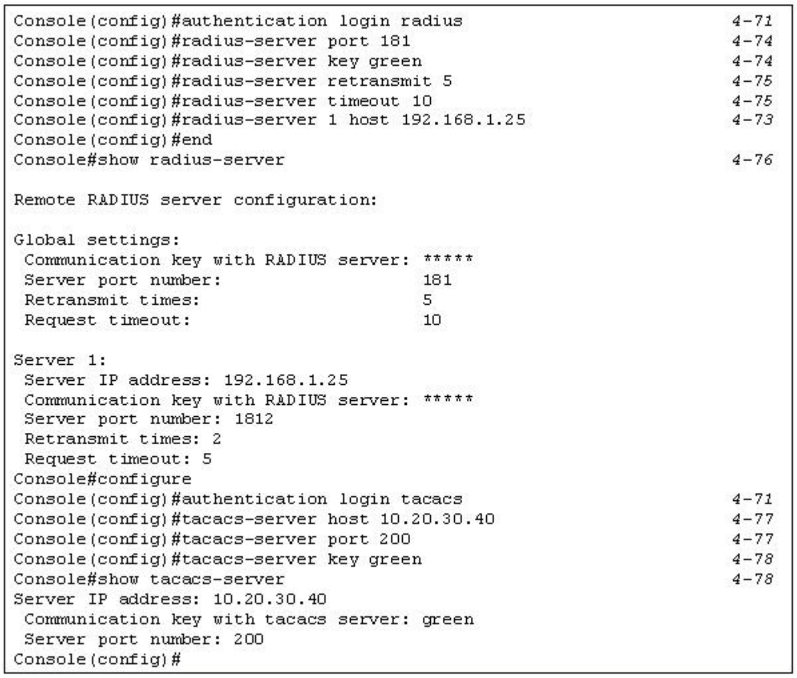
TACACS Settings:

Server IP Address	10.11.12.13
Server Port Number (1-65535)	49
Secret Text String	

FIG. 52 Web - Authentication Settings

Authentication Settings - CLI

Specify all the required parameters to enable logon authentication.



```
Console(config)#authentication login radius                          4-71
Console(config)#radius-server port 181                               4-74
Console(config)#radius-server key green                              4-74
Console(config)#radius-server retransmit 5                           4-75
Console(config)#radius-server timeout 10                            4-75
Console(config)#radius-server 1 host 192.168.1.25                    4-73
Console(config)#end
Console#show radius-server                                           4-76

Remote RADIUS server configuration:

Global settings:
 Communication key with RADIUS server: *****
 Server port number:                   181
 Retransmit times:                     5
 Request timeout:                      10

Server 1:
 Server IP address: 192.168.1.25
 Communication key with RADIUS server: *****
 Server port number: 1812
 Retransmit times: 2
 Request timeout: 5
Console#configure
Console(config)#authentication login tacacs                          4-71
Console(config)#tacacs-server host 10.20.30.40                       4-77
Console(config)#tacacs-server port 200                               4-77
Console(config)#tacacs-server key green                              4-78
Console#show tacacs-server                                           4-78
Server IP address: 10.20.30.40
 Communication key with tacacs server: green
 Server port number: 200
Console(config)#
```

FIG. 53 CLI - Authentication Settings

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.

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.
- 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 and Netscape Navigator 4.x or above.

HTTPS Support

The following web browsers and operating systems currently support HTTPS:

HTTPS Support	
• **Internet Explorer 5.0 or later:**	• Windows 98 • Windows NT (with service pack 6a) • Windows 2000 • Windows XP
• **Netscape Navigator 4.76 or later:**	• Windows 98 • Windows NT (with service pack 6a) • Windows 2000 • Windows XP • Solaris 2.6

Command Attributes

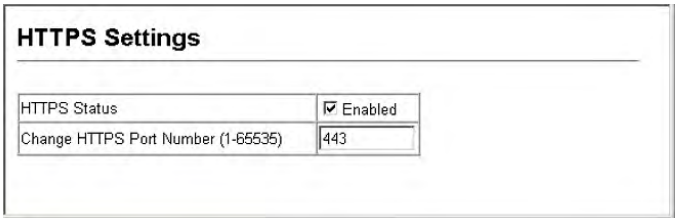
To specify a secure-site certificate, see *Replacing the Default Secure-Site Certificate* section on page 60.

Command Attributes	
• **Internet Explorer 5.0 or later:**	• Windows 98 • Windows NT (with service pack 6a) • Windows 2000 • Windows XP
• **Netscape Navigator 4.76 or later:**	• Windows 98 • Windows NT (with service pack 6a) • Windows 2000 • Windows XP • Solaris 2.6

- **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/SSL connection to the switch's web interface (default: Port 443).

Configuring HTTPS - Web

Click *Security*, *HTTPS Settings*. *Enable HTTPS* and specify the port number, then click **Apply**.



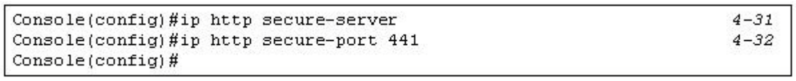
HTTPS Settings

HTTPS Status	☑ Enabled
Change HTTPS Port Number (1-65535)	443

FIG. 54 Web - HTTPS Settings

Configuring HTTPS - CLI

CLI – This example enables the HTTP secure server and modifies the port number.



```
Console(config)#ip http secure-server                                        4-31
Console(config)#ip http secure-port 441                                      4-32
Console(config)#
```

FIG. 55 CLI - HTTPS Settings

Replacing the Default Secure-Site Certificate

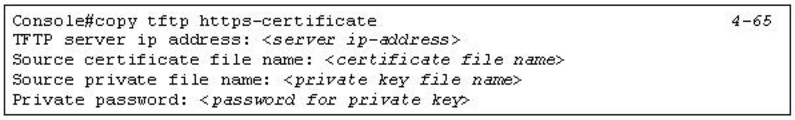
When you log onto the web interface using HTTPS (for secure access), a Secure Sockets Layer (SSL) certificate appears for the switch. By default, the certificate that Netscape and Internet Explorer display will be associated with a warning that the site is not recognized as a secure site. This is because 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 use the following command at the switch's command-line interface to replace the default (unrecognized) certificate with an authorized one:



```
Console#copy tftp https-certificate                                          4-65
TFTP server ip address: <server ip-address>
Source certificate file name: <certificate file name>
Source private file name: <private key file name>
Private password: <password for private key>
```

FIG. 56 CLI - Replacing the default Secure-Site Certificate

NOTE

The switch must be reset for the new certificate to be activated. To reset the switch, type: ***Console#reload***

Configuring the Secure Shell

The Berkley-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 Berkley 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 that 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.

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 55).

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 15684995401867669259333946775054617325313674890836547254
   15020245593199868544358361651999923329781766065830956 10825913212890233
   76546801726272571413428762941301196195566782 595664104869574278881462065
   194174677298486546861571773939016477935594230357741309802273708779454524083971
   75264635805817671670957480477611 7
   ```

3. *Import Client's Public Key to the Switch* – Use the **copy tftp public-key** command (page 233) 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 55.) 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 1341081685609893921040944920155425347631641921872958921143173880
   055536161631051775940838686311092912322268285192543746031009371877211996963178
   136627741416898513204911720483033925432410163799759237144901193800609025394840
   848271781943722884025331159521348610229029789827213532671316294325328189150453
   06393916643 steve@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. *Challenge-Response 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. The following exchanges take place during this process:
   a. The client sends its 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 the public key to encrypt a random sequence of bytes, and sends this string to the client.
   d. The client uses its private key to decrypt the bytes, and sends the decrypted bytes back to the switch.

e. The switch compares the decrypted bytes to the original bytes it sent. If the two sets match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

NOTE

1. *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.*
2. *The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.*

Generating the Host Key Pair

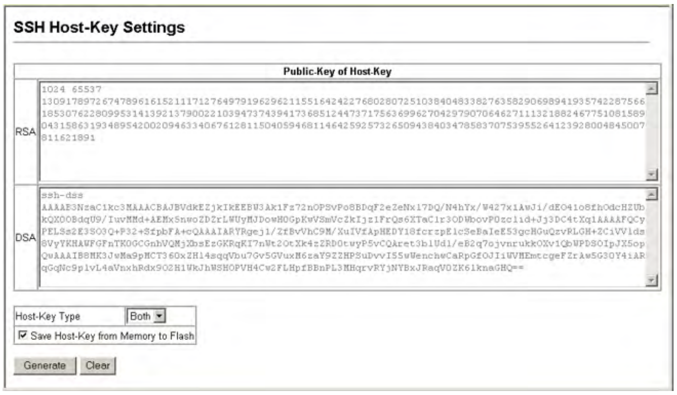
A host public/private key pair is used to provide secure communications between an SSH client and the switch. After generating this key pair, you must provide the host public key to SSH clients and import the client’s public key to the switch as described in the proceeding section (Command Usage).

Field Attributes

Field Attributes	
• **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 (Version2): 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: RSA) 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.
• **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.
• **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.

Configuring the Secure Shell - Web

Click *Security*, *SSH*, *Host-Key Settings*. Select the host-key type from the drop-down box, select the option to save the host key from memory to flash (if required) prior to generating the key, and then click **Generate**.



SSH Host-Key Settings

Public-Key of Host-Key

RSA

```
1024 65537
1309178972674789616152111712764979196296211551642422768028072510384048338276358290698941935742287566
1853076228099531413921379002210394737439417368512447371756369962704297907064627111321882467751081589
0431586319348954200209463340676128115040594681146425925732650943840347858370753955264123928004845007
811621891
```

DSA

```
ssh-dss
AAAAB3NzaC1kc3MAAACBAJBVdkEZjkIkEEBU3Ak1Fz72nOPSvPo8BDqF2eZeNx17DQ/N4hYx/W427x1AwJi/dEO41o8fhOdcHZUb
kQXOOBdqU9/IuvMMd+AEMx5nwoZDZrLWUyMJDowH0GpKwVSmVcZkIjz1FrQs6XTaC1r3ODWbovP0zc1id+Jj3DC4tXq1AAAAFQCy
PELSs2E3SO3Q+P32+SfpbFA+cQAAAIARYRgej1/ZfBvVhC9M/XuIVfApHEDY18fcrzpE1cSeBaIeE53gcHGuQzvRLGH+ZCiVV1ds
8VyYKHAWFGFnTK0GCGnhVQMjXbsEzGKRqKI7nWt2OtXk4zZRD0twyP5vCQAret3b1Ud1/eB2q7ojvnrukk0Xv1QbWPDSOIpJX5op
QwAAAIB8MK3JwMa9pMCT360xZH14sqqVbu7Gv5GVuxM6zaY9ZZHPSuDvvI55wWenchwCaRpGfOJIiWVMEmtcgeFZrAw5G3OY4iAR
qGqNc9plvL4aVnxhRdx9O2H1WkJhWSHOPVH4Cw2FLHpfBBnPL3MHqrvRYjNYBxJRaqV0ZK61knaGHQ==
```

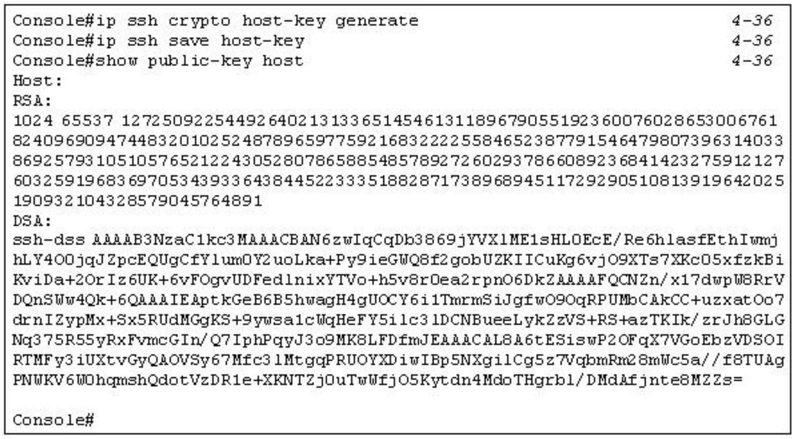
Host-Key Type: Both

☑ Save Host-Key from Memory to Flash

FIG. 57 Web - SSH Host-Key Settings

Configuring the Secure Shell - CLI

This example generates a host-key pair using both the RSA and DSA algorithms, stores the keys to flash memory, and then displays the host's public keys.



```
Console#ip ssh crypto host-key generate                         4-36
Console#ip ssh save host-key                                    4-36
Console#show public-key host                                    4-36
Host:
RSA:
1024 65537 127250922544926402131336514546131189679055192360076028653006761
82409690947448320102524878965977592168322225584652387791546479807396314033
86925793105105765212243052807865885485789272602937866089236841423275912127
60325919683697053439336438445223335188287173896894511729290510813919642025
190932104328579045764891
DSA:
ssh-dss AAAAB3NzaC1kc3MAAACBAN6zwIqCqDb3869jYVX1ME1sHLOEcE/Re6hlasfEthIwmj
hLY4O0jqJZpcEQUgCfYlum0Y2uoLka+Py9ieGWQ8f2gobUZKIICuKg6vjO9XTs7XKc05xfzkBi
KviDa+2OrIz6UK+6vFOgvUDFedlnixYTVo+h5v8r0ea2rpnO6DkZAAAAFQCNZn/x17dwpW8RrV
DQnSWw4Qk+6QAAAIEAptkGeB6B5hwagH4gUOCY6i1TmrmSiJgfwO9OqRPUMbCAkCC+uzxatOo7
drnIZypMx+Sx5RUdMGgKS+9ywsa1cWqHeFY5ilc31DCNBueeLykZzVS+RS+azTKIk/zrJh8GLG
Nq375R55yRxFvmcGIn/Q7IphPqyJ3o9MK8LFDfmJEAAACAL8A6tESiswP2OFqX7VGoEbzVDSOI
RTMFy3iUXtvGyQAOVSy67Mfc31MtgqPRUOYXDiwIBp5NXgilCg5z7VqbmRm28mWc5a//f8TUAg
PNWKV6W0hqmshQdotVzDR1e+XKNTZjOuTwWfjO5Kytdn4MdoTHgrbl/DMdAfjnte8MZZs=

Console#
```

FIG. 58 CLI - SSH Host-Key Settings

Configuring the SSH Server

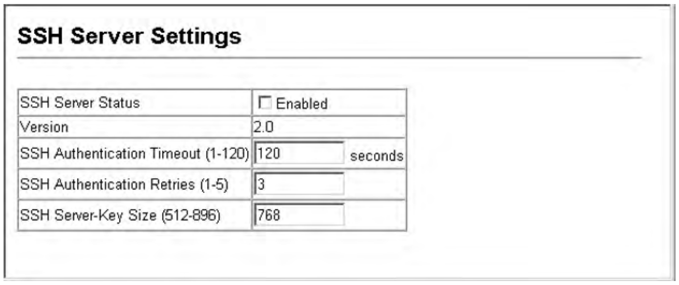
The SSH server includes basic settings for authentication.

Field Attributes

Field Attributes	
• **SSH Server Status:**	Allows you to enable/disable the SSH server feature 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 to 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) • 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.

Configuring the SSH Server - Web

Click *Security*, *SSH*, *Settings*. *Enable SSH* and adjust the authentication parameters as required, then click Apply. Note that you must first generate the host key pair on the SSH Host-Key Settings page before you can enable the SSH server.



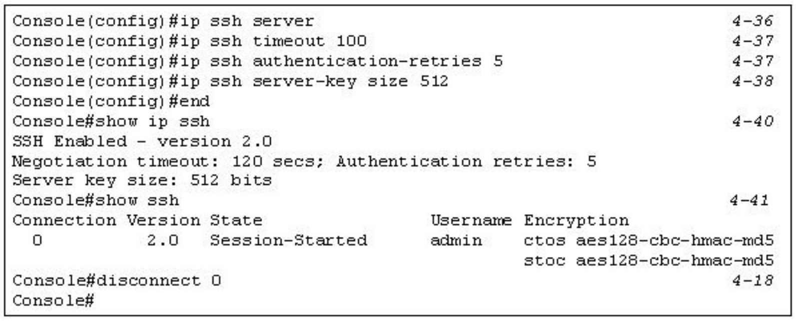
SSH Server Settings

SSH Server Status	□ Enabled
Version	2.0
SSH Authentication Timeout (1-120)	120 seconds
SSH Authentication Retries (1-5)	3
SSH Server-Key Size (512-896)	768

FIG. 59 Web - SSH Server Settings

Configuring the SSH Server - CLI

This example enables SSH, sets the authentication parameters, and displays the current configuration. It shows that the administrator has made a connection via SHH, and then disables this connection.



```
Console(config)#ip ssh server                                             4-36
Console(config)#ip ssh timeout 100                                        4-37
Console(config)#ip ssh authentication-retries 5                           4-37
Console(config)#ip ssh server-key size 512                                4-38
Console(config)#end
Console#show ip ssh                                                       4-40
SSH Enabled - version 2.0
Negotiation timeout: 120 secs; Authentication retries: 5
Server key size: 512 bits
Console#show ssh                                                          4-41
Connection Version State                  Username Encryption
  0          2.0    Session-Started       admin    ctos aes128-cbc-hmac-md5
                                                   stoc aes128-cbc-hmac-md5
Console#disconnect 0                                                      4-18
Console#
```

FIG. 60 CLI - SSH Server Settings

Configuring Port Security

Port security is a feature that allows you 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. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted as 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, first allow the switch to dynamically learn the <source MAC address, VLAN> pair for frames received on a port for an initial training period, and then enable port security to stop address learning. Be sure you enable the learning function long enough to ensure that all valid VLAN members have been registered on the selected port. Note that you can also restrict the maximum number of addresses that can be learned by a port.

To add new VLAN members at a later time, you can manually add secure addresses with the Static Address Table (see the *Address Table Settings* section on page 109), or turn off port security to re-enable the learning function long enough for new VLAN members to be registered. Learning may then be disabled again, if desired, for security.

Command Usage

A secure port has the following restrictions:

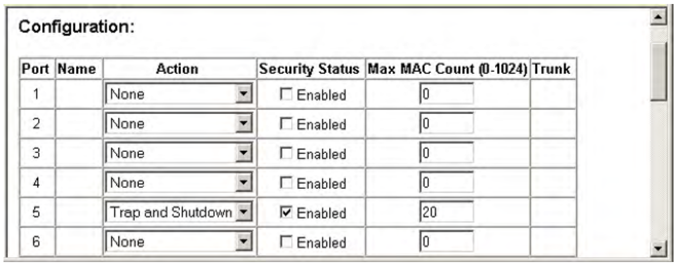
- Cannot use port monitoring.
- Cannot be a multi-VLAN port.
- It cannot be used as a member of a static or dynamic trunk.
- It should not be connected to a network interconnection device.
- If a port is disabled (shut down) due to a security violation, it must be manually re-enabled from the *Port/Port Configuration* page (see the *Port Configuration* section on page 85).

Command Attributes

Command Attributes	
• **Port:**	Port number.
• **Name:**	Descriptive text.
• **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)
• **Trunk:**	Trunk number if port is a member (see the *Creating Trunk Groups* section on page 88).

Configuring Port Security - Web

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



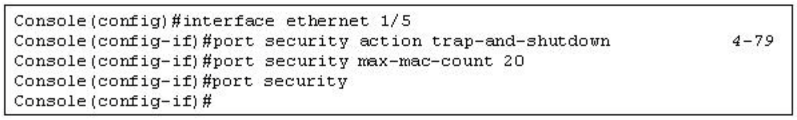
Configuration:

Port	Name	Action	Security Status	Max MAC Count (0-1024)	Trunk
1		None	□ Enabled	0	
2		None	□ Enabled	0	
3		None	□ Enabled	0	
4		None	□ Enabled	0	
5		Trap and Shutdown	☑ Enabled	20	
6		None	□ Enabled	0	

FIG. 61 Web - Configuring Port Security

Configuring Port Security - CLI

This example enables port security for Port 5 with the intrusion action to send a trap and disable the port, and then sets the maximum addresses to learn on the port to 20.



```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap-and-shutdown          4-79
Console(config-if)#port security max-mac-count 20
Console(config-if)#port security
Console(config-if)#
```

FIG. 62 Web - 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.

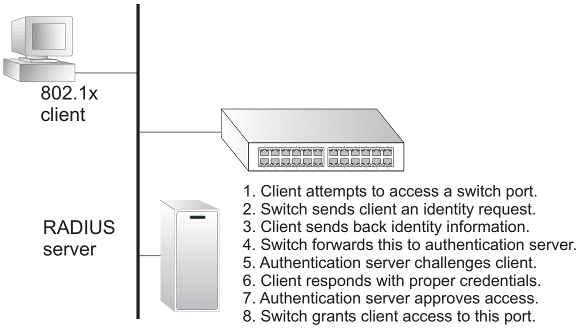

802.1x
client
RADIUS
server
1. Client attempts to access a switch port.
2. Switch sends client an identity request.
3. Client sends back identity information.
4. Switch forwards this to authentication server.
5. Authentication server challenges client.
6. Client responds with proper credentials.
7. Authentication server approves access.
8. Switch grants client access to this port.

FIG. 63 802.1x Port Authentication

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 authentication method must be MD5. 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, network access is denied and the port remains blocked.

Requirements

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.
- Dot1x 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. (Some clients have native support in Windows, otherwise the dot1x client must support it).

Displaying and Configuring the 802.1x Global Setting

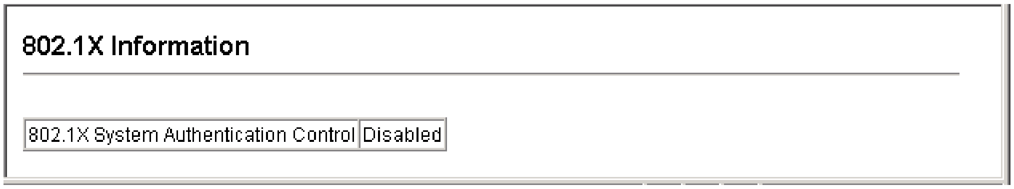
The 802.1x protocol must be enabled globally for the switch system before port settings are active.

Command Attributes

Command Attributes	
• **802.1x System Authentication Control:**	The global setting for 802.1x. • Default: Disabled

Displaying and Configuring the 802.1x Global Setting - Web

To display the current global setting for 802.1x, click *Security*, *802.1X*, *Information*.



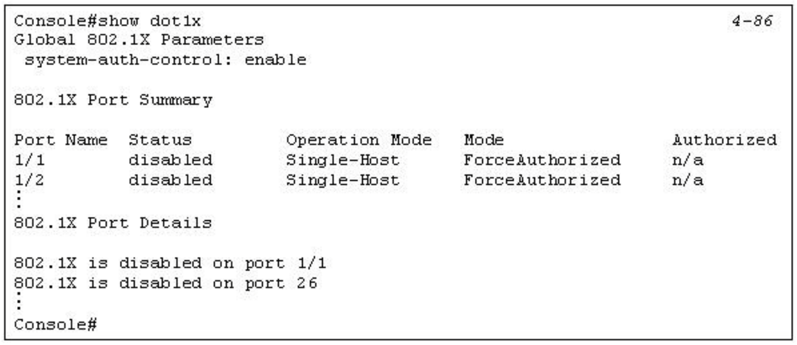
802.1X Information

802.1X System Authentication Control	Disabled

FIG. 64 Web - 802.1X Information

Displaying and Configuring the 802.1x Global Setting - CLI

This example enables 802.1x globally for the switch and shows the current setting.



```
Console#show dot1x                                                    4-86
Global 802.1X Parameters
 system-auth-control: enable

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
:
802.1X Port Details

802.1X is disabled on port 1/1
802.1X is disabled on port 26
:
Console#
```

FIG. 65 CLI - 802.1X Information

Configuring Port Settings for 802.1x

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. These parameters are described in this section.

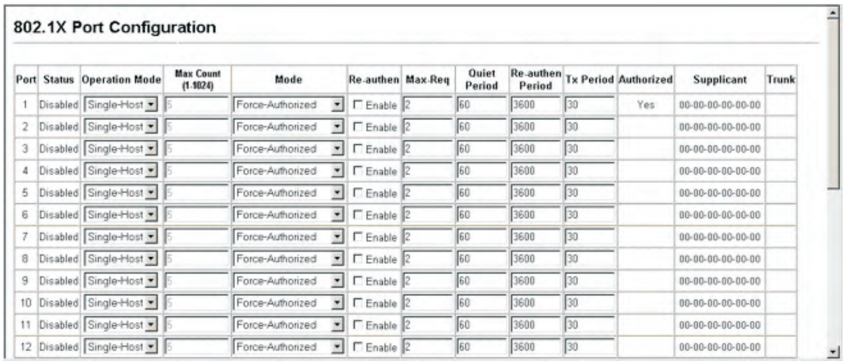
Command Attributes

Command Attributes	
• **Status:**	Indicates if authentication is enabled or disabled on the port.
• **Operation Mode:**	Allows single or multiple hosts (clients) to connect to an 802.1X-authorized port. • Range: Single-Host, Multi-Host • Default: Single-Host
• **Max 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

Command Attributes (Cont.)	
• **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
• **Authorized:**	• Yes – Connected client is authorized. • No – Connected client is not authorized. • *Blank* – Displays nothing when dot1x is disabled on a port.
• **Supplicant:**	Indicates the MAC address of a connected client.
• **Trunk:**	Indicates if the port is configured as a trunk port.

Configuring Port Settings for 802.1x - Web

Click *Security*, *802.1x*, *Port Configuration*. Modify the parameters required, and click **Apply**.



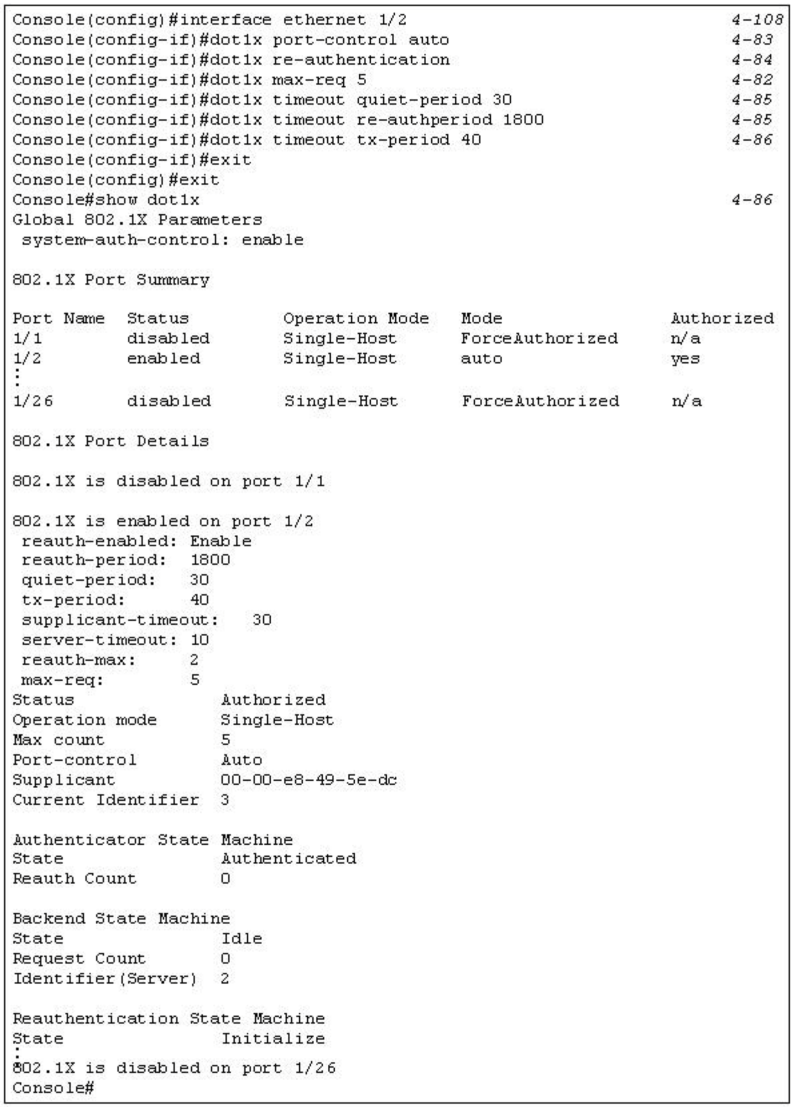
802.1X Port Configuration

Port	Status	Operation Mode	Max Count (1-1024)	Mode	Re-authen	Max-Req	Quiet Period	Re-authen Period	Tx Period	Authorized	Supplicant	Trunk
1	Disabled	Single-Host	5	Force-Authorized	□ Enable	2	60	3600	30	Yes	00-00-00-00-00-00	
2	Disabled	Single-Host	5	Force-Authorized	□ Enable	2	60	3600	30		00-00-00-00-00-00	
3	Disabled	Single-Host	5	Force-Authorized	□ Enable	2	60	3600	30		00-00-00-00-00-00	
4	Disabled	Single-Host	5	Force-Authorized	□ Enable	2	60	3600	30		00-00-00-00-00-00	
5	Disabled	Single-Host	5	Force-Authorized	□ Enable	2	60	3600	30		00-00-00-00-00-00	
6	Disabled	Single-Host	5	Force-Authorized	□ Enable	2	60	3600	30		00-00-00-00-00-00	
7	Disabled	Single-Host	5	Force-Authorized	□ Enable	2	60	3600	30		00-00-00-00-00-00	
8	Disabled	Single-Host	5	Force-Authorized	□ Enable	2	60	3600	30		00-00-00-00-00-00	
9	Disabled	Single-Host	5	Force-Authorized	□ Enable	2	60	3600	30		00-00-00-00-00-00	
10	Disabled	Single-Host	5	Force-Authorized	□ Enable	2	60	3600	30		00-00-00-00-00-00	
11	Disabled	Single-Host	5	Force-Authorized	□ Enable	2	60	3600	30		00-00-00-00-00-00	
12	Disabled	Single-Host	5	Force-Authorized	□ Enable	2	60	3600	30		00-00-00-00-00-00	

FIG. 66 Web - 802.1x Port Configuration

Configuring Port Settings for 802.1x - CLI

This example sets the 802.1x parameters on port 2. For a description of the additional fields displayed in this example, see *show dot1x* section on page 259.



```
Console(config)#interface ethernet 1/2                                    4-108
Console(config-if)#dot1x port-control auto                                4-83
Console(config-if)#dot1x re-authentication                                4-84
Console(config-if)#dot1x max-req 5                                        4-82
Console(config-if)#dot1x timeout quiet-period 30                          4-85
Console(config-if)#dot1x timeout re-authperiod 1800                       4-85
Console(config-if)#dot1x timeout tx-period 40                             4-86
Console(config-if)#exit
Console(config)#exit
Console#show dot1x                                                        4-86
Global 802.1X Parameters
 system-auth-control: enable

802.1X Port Summary

Port Name  Status         Operation Mode   Mode               Authorized
1/1        disabled       Single-Host      ForceAuthorized    n/a
1/2        enabled        Single-Host      auto               yes
:
1/26       disabled       Single-Host      ForceAuthorized    n/a

802.1X Port Details

802.1X is disabled on port 1/1

802.1X is enabled on port 1/2
 reauth-enabled:  Enable
 reauth-period:   1800
 quiet-period:    30
 tx-period:       40
 supplicant-timeout:    30
 server-timeout:  10
 reauth-max:      2
 max-req:         5
Status               Authorized
Operation mode       Single-Host
Max count            5
Port-control         Auto
Supplicant           00-00-e8-49-5e-dc
Current Identifier   3

Authenticator State Machine
State                Authenticated
Reauth Count         0

Backend State Machine
State                Idle
Request Count        0
Identifier(Server)   2

Reauthentication State Machine
State                Initialize
:
802.1X is disabled on port 1/26
Console#
```

FIG. 67 CLI - 802.1x Port Configuration

Displaying 802.1x Statistics

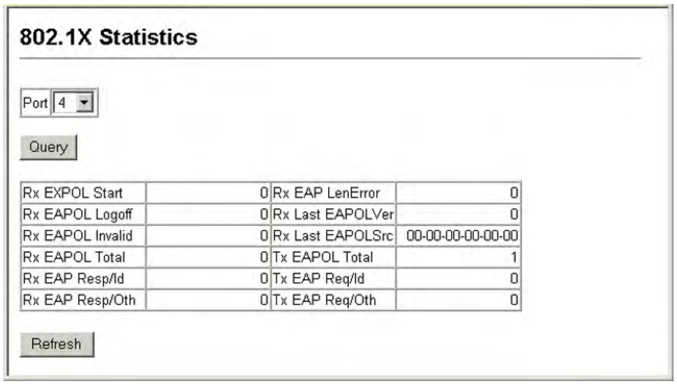
This switch can display statistics for dot1x protocol exchanges for any port.

802.1x Statistics	
Parameter	**Description**
Rx EXPOL 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 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.
Rx Last EAPOLVer	The protocol version number carried in the most recently received EAPOL frame.
Rx Last EAPOLSrc	The source MAC address carried in the most recently received EAPOL frame.
Tx EAPOL Total	The number of EAPOL frames of any type that have been transmitted by this Authenticator.
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.

Displaying 802.1x Statistics - Web

Select *Security*, *802.1x*, *Statistics*. Select the required port and then click **Query**.

Click **Refresh** to update the statistics.



802.1X Statistics

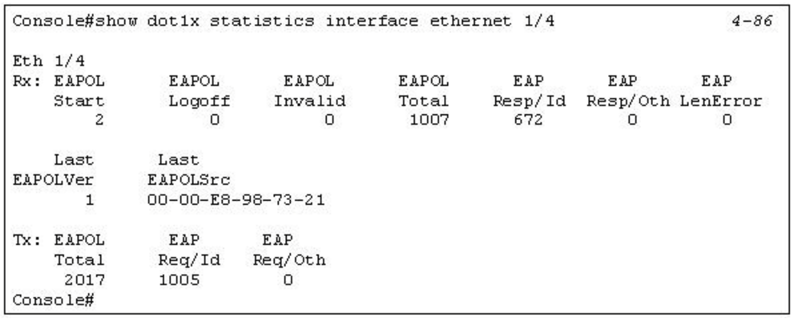
Port 4

Rx EXPOL Start	0	Rx EAP LenError	0
Rx EAPOL Logoff	0	Rx Last EAPOLVer	0
Rx EAPOL Invalid	0	Rx Last EAPOLSrc	00-00-00-00-00-00
Rx EAPOL Total	0	Tx EAPOL Total	1
Rx EAP Resp/Id	0	Tx EAP Req/Id	0
Rx EAP Resp/Oth	0	Tx EAP Req/Oth	0

FIG. 68 Web - Displaying 802.1x Statistics

Displaying 802.1x Statistics - CLI

This example displays the 802.1x statistics for port 4.



```
Console#show dot1x statistics interface ethernet 1/4                   4-86

Eth 1/4
Rx: EAPOL      EAPOL      EAPOL      EAPOL      EAP      EAP      EAP
    Start      Logoff     Invalid    Total      Resp/Id  Resp/Oth LenError
        2          0          0       1007      672          0        0

    Last       Last
EAPOLVer      EAPOLSrc
       1      00-00-E8-98-73-21

Tx: EAPOL      EAP       EAP
    Total      Req/Id    Req/Oth
     2017      1005         0
Console#
```

FIG. 69 CLI - Displaying 802.1x Statistics

Filtering Addresses for SNMP Client Access

The switch allows you to create a list of up to 16 IP addresses or IP address groups that are allowed access to the switch via SNMP management software.

Command Usage

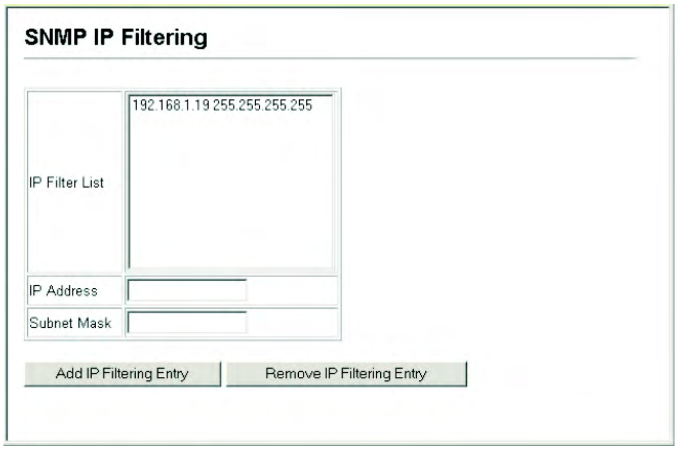
- To specify the clients allowed SNMP access, enter an IP address along with a subnet mask to identify a specific host or a range of valid addresses. For example:
  - IP address 192.168.1.1 and mask 255.255.255.255 – Specifies a valid IP address of 192.168.1.1 for a single client.
  - IP address 192.168.1.1 and mask 255.255.255.0 – Specifies a valid IP address group from 192.168.1.0 to 192.168.1.254.
- IP filtering only restricts management access for clients running SNMP management software such as HP OpenView. It does not affect management access to the switch using the web interface or Telnet.
- The default setting is null, which allows all IP groups SNMP access to the switch. If one or more IP addresses are configured, IP filtering is enabled and only addresses listed in this table will have SNMP access.

Command Attributes

Command Attributes	
• IP Filter List:	Displays a list of the IP address/subnet mask entries currently configured for SNMP access.
• IP address:	Specifies a new IP address to add to the IP Filter List.
• Subnet Mask:	Specifies a single IP address or group of addresses. If the IP is the address of a single management station, set the mask to 255.255.255.255. Otherwise, an IP address group will be specified by any other mask.

Filtering Addresses for SNMP Client Access - Web

Click *SNMP*, *SNMP IP Filtering*. To add a client, enter the new address, the subnet mask for a node or an address range, and then click “**Add IP Filtering Entry**.”



SNMP IP Filtering

IP Filter List	192.168.1.19 255.255.255.255
IP Address	
Subnet Mask	

FIG. 70 Filtering Addresses for SNMP Access

Filtering Addresses for SNMP Client Access - CLI

This example allows SNMP access for a specific client.

```
Console(config)#snmp ip filter 10.1.2.3 255.255.255.255
Console(config)#
```

Configuring ACLs

Overview

Access Control Lists (ACL) provide packet filtering for IP frames (based on address, protocol, Layer 4 protocol port number or TCP control code) or any frames (based on MAC address or Ethernet type). To filter incoming packets, first create an access list, add the required rules, specify a mask to modify the precedence in which the rules are checked, 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 or egress 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 for a list of all permit rules, the packet is dropped; and if no rules match for a list of all deny rules, the packet is accepted.

Command Usage

The following restrictions apply to ACLs:

- Each ACL can have up to 32 rules.
- The maximum number of ACLs is also 32.
- However, due to resource restrictions, the average number of rules bound to the ports should not exceed 20.
- You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.
- When an ACL is bound to an interface as an egress filter, all entries in the ACL must be deny rules. Otherwise, the bind operation will fail.
- The switch does not support the explicit “deny any” rule for the egress IP ACL or the egress MAC ACLs. If these rules are included in ACL, and you attempt to bind the ACL to an interface for egress checking, the bind operation will fail.

The order in which active ACLs are checked is as follows:

1. User-defined rules in the Egress MAC ACL for egress ports.
2. User-defined rules in the Egress IP ACL for egress ports.
3. User-defined rules in the Ingress MAC ACL for ingress ports.
4. User-defined rules in the Ingress IP ACL for ingress ports.
5. Explicit default rule (permit any) in the ingress IP ACL for ingress ports.
6. Explicit default rule (permit any) in the ingress MAC ACL for ingress ports.
7. If no explicit rule is matched, the implicit default is permit all.

Setting the ACL Name and Type

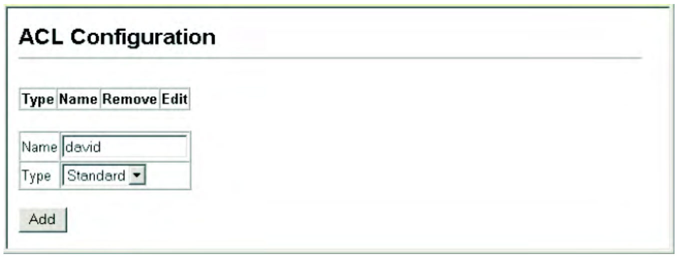
Use the ACL Configuration page to designate the name and type of an ACL.

Command Attributes

Command Attributes	
• **Name:**	Name of the ACL. (Maximum length: 16 characters)
• **Type:**	There are three filtering modes: • Standard: IP ACL mode that filters packets based on the source IP address. • Extended: IP ACL mode that filters packets based on source or destination IP address, as well as protocol type and protocol port number. If the “TCP” protocol is specified, then you can also filter packets based on the TCP control code. • MAC: MAC ACL mode that filters packets based on the source or destination MAC address and the Ethernet frame type (RFC 1060).

Setting the ACL Name and Type - Web

Click *Security*, *ACL*, *ACL Configuration*. Enter an ACL name in the Name field, select the list type (IP Standard, IP Extended, or MAC), and click **Add** to open the configuration page for the new list.



ACL Configuration

Type	Name	Remove	Edit

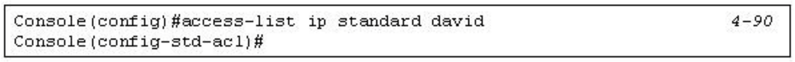
Name: david

Type: Standard

FIG. 71 Web - Selecting ACL Type

Setting the ACL Name and Type - CLI

This example creates a standard IP ACL named *bill*.



```
Console(config)#access-list ip standard david                         4-90
Console(config-std-acl)#
```

FIG. 72 CLI - Selecting ACL Type

Configuring a Standard IP ACL

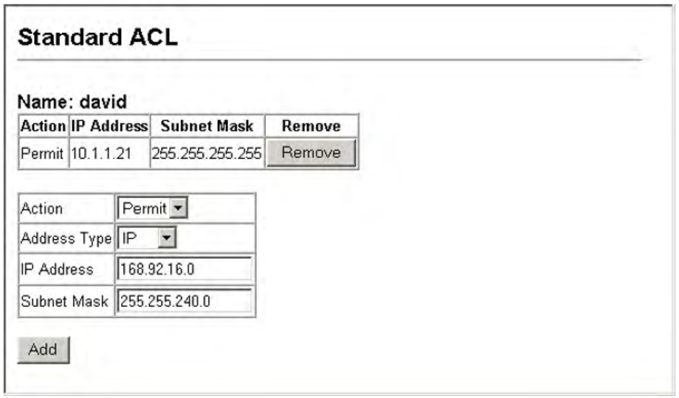
Command Attributes

Command Attributes	
• **Action:**	An ACL can contain permit rules, deny rules, or a combination of both. • Default: Permit rules
• **Address Type:**	Specifies the filter type - Any, Host, or IP. • Default: Any
• **IP Address:**	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 Address and SubMask fields. • Options: Any, Host, IP • Default: Any
• **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.

Configuring a Standard IP ACL - Web

Specify the action (i.e., *Permit* or *Deny*). Select the address type (*Any*, *Host*, or *IP*).

- If you select "**Host**," enter a specific address. I
- If you select "**IP**," enter a subnet address and the mask for an address range. Then click **Add**.



Standard ACL

Name: david

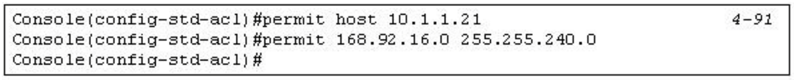
Action	IP Address	Subnet Mask	Remove
Permit	10.1.1.21	255.255.255.255	Remove

Action	Permit
Address Type	IP
IP Address	168.92.16.0
Subnet Mask	255.255.240.0

FIG. 73 Web - Configuring Standard ACLs

Configuring a Standard IP ACL - CLI

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                          4-91
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

FIG. 74 CLI - Configuring Standard ACLs

Configuring an Extended IP ACL

Command Attributes

Command Attributes	
• **Action:**	An ACL can contain permit rules, deny rules or a combination of both. • Default: Permit 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 SubMask 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 SubMask on page 74.)
• **Service Type:**	Packet priority settings based on the following criteria: • Precedence – IP precedence level. (Range: 0-7) • TOS – Type of Service level. (Range: 0-15) • DSCP – DSCP priority level. (Range: 0-64)
• **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

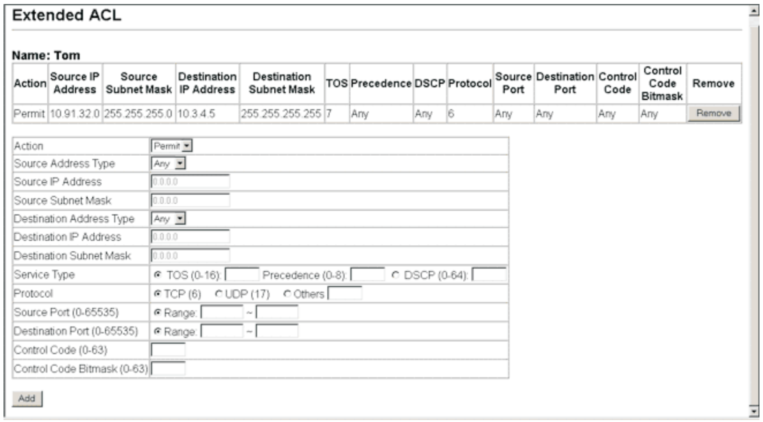
Command Attributes (Cont.)	
• **Source/Destination Port Bitmask:**	Decimal number representing the port bits to match. • Range: 0-65535
• **Control Code:**	Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. • Range: 0-63
• **Control Code Bitmask:**	Decimal number representing the code bits to match. The control bitmask 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 bitmask 2 • Both SYN and ACK valid, use control-code 18, control bitmask 18 SYN valid and ACK invalid, use control-code 2, control bitmask 18

Configuring an Extended IP ACL - Web

Specify the action (i.e., *Permit* or *Deny*). Specify the source and/or destination addresses. Select the address type (*Any*, *Host*, or *IP*).

- If you select "Host," enter a specific address.
- If you select "IP," enter a subnet address and the mask for an address range.

Set any other required criteria, such as service type, protocol type, or TCP control code. Then click **Add**.



Extended ACL

Name: Tom

Action	Source IP Address	Source Subnet Mask	Destination IP Address	Destination Subnet Mask	TOS	Precedence	DSCP	Protocol	Source Port	Destination Port	Control Code	Control Code Bitmask	Remove
Permit	10.91.32.0	255.255.255.0	10.3.4.5	255.255.255.255	7	Any	Any	6	Any	Any	Any	Any	Remove

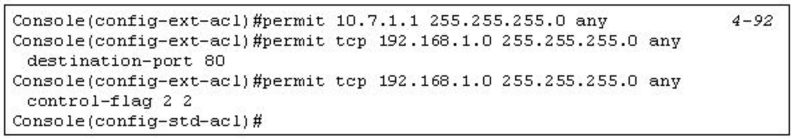
Action	Permit
Source Address Type	Any
Source IP Address	0.0.0.0
Source Subnet Mask	0.0.0.0
Destination Address Type	Any
Destination IP Address	0.0.0.0
Destination Subnet Mask	0.0.0.0
Service Type	● TOS (0-16): Precedence (0-8): ○ DSCP (0-64):
Protocol	● TCP (6) ○ UDP (17) ○ Others
Source Port (0-65535)	● Range: ~
Destination Port (0-65535)	● Range: ~
Control Code (0-63)	
Control Code Bitmask (0-63)	

FIG. 75 Configuring Extended ACLs

Configuring an Extended IP ACL - CLI

This example adds three rules:

1. Accept any incoming packets if the source address is in 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.
2. Allow TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (i.e., HTTP).
3. Permit all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to "SYN."



```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any          4-92
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any
  destination-port 80
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any
  control-flag 2 2
Console(config-std-acl)#
```

FIG. 76 Configuring Extended ACLs

Configuring a MAC ACL

Command Attributes

Command Attributes	
• **Action:**	An ACL can contain permit rules, deny rules, or a combination of both. (Default: Permit 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 Bitmask fields. • Options: Any, Host, MAC • Default: Any
• **Source/Destination MAC Address:**	Source or destination MAC address.
• **Source/Destination Bitmask:**	Hexadecimal mask for source or destination MAC address.
• **VID:**	VLAN ID. (Range: 1-4095)
• **VID Mask:**	VLAN bitmask. (Range: 1-4095)
• **Ethernet Type:**	This option can only be used to filter Ethernet II formatted packets. • Range: 600-fff 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 Bitmask:**	Protocol bitmask. (Range: 600-fff 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.
• **Packet Format Bitmask:**	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.

Command Usage

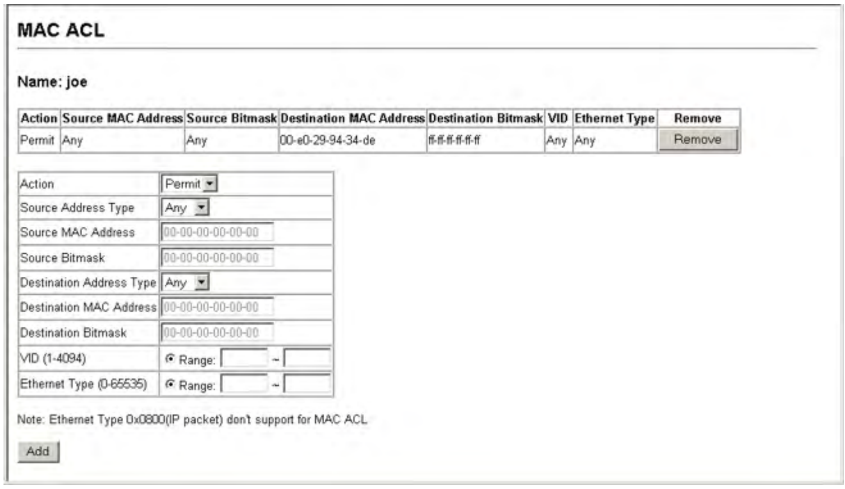
Egress MAC ACLs only work for destination-mac-known packets, not for multicast, broadcast, or destination-mac-unknown packets.

Configuring a MAC ACL - Web

Specify the action (i.e., *Permit* or *Deny*). Specify the source and/or destination addresses. Select the address type (*Any*, *Host*, or *MAC*).

- 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 bitmask for an address range.

Set any other required criteria, such as VID, Ethernet type, or packet format. Then click **Add**.



MAC ACL

Name: joe

Action	Source MAC Address	Source Bitmask	Destination MAC Address	Destination Bitmask	VID	Ethernet Type	Remove
Permit	Any	Any	00-e0-29-94-34-de	ff-ff-ff-ff-ff-ff	Any	Any	Remove

Action	Permit
Source Address Type	Any
Source MAC Address	00-00-00-00-00-00
Source Bitmask	00-00-00-00-00-00
Destination Address Type	Any
Destination MAC Address	00-00-00-00-00-00
Destination Bitmask	00-00-00-00-00-00
VID (1-4094)	● Range: ~
Ethernet Type (0-65535)	● Range: ~

Note: Ethernet Type 0x0800(IP packet) don't support for MAC ACL

FIG. 77 Web - Configuring MAC ACLs

Configuring a MAC ACL - CLI

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                                                      4-98
Console(config-mac-acl)#
```

FIG. 78 CLI - Configuring MAC ACLs

Configuring ACL Masks

You can specify optional masks that control the order in which ACL rules are checked. The switch includes two system default masks that pass/filter packets matching the permit/deny rules specified in an ingress ACL. You can also configure up to seven user-defined masks for an ingress or egress ACL. A mask must be bound exclusively to one of the basic ACL types (i.e., Ingress IP ACL, Egress IP ACL, Ingress MAC ACL or Egress MAC ACL), but a mask can be bound to up to four ACLs of the same type.

Command Usage

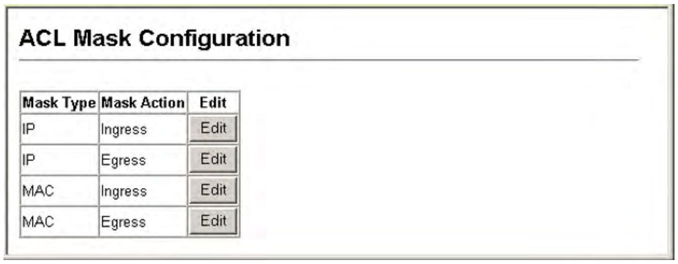
- Up to seven entries can be assigned to an ACL mask.
- Packets crossing a port are checked against all the rules in the ACL until a match is found. The order in which these packets are checked is determined by the mask, and not the order in which the ACL rules are entered.
- First create the required ACLs and the ingress or egress masks before mapping an ACL to an interface.
- You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.

Specifying the Mask Type

Use the *ACL Mask Configuration* page to edit the mask for the Ingress IP ACL (*Egress IP ACL*, *Ingress MAC ACL* or *Egress MAC ACL*).

Configuring ACL Masks - Web

Click *Security*, *ACL*, *ACL Mask Configuration*. Click **Edit** for one of the basic mask types to open the configuration page.



ACL Mask Configuration

Mask Type	Mask Action	Edit
IP	Ingress	Edit
IP	Egress	Edit
MAC	Ingress	Edit
MAC	Egress	Edit

FIG. 79 Web - ACL Mask Configuration

Configuring ACL Masks - CLI

This example creates an IP ingress mask, and then adds two rules. Each rule is checked in order of precedence to look for a match in the ACL entries. The first entry matching a mask is applied to the inbound packet.

```
Console(config)#access-list ip mask-precedence in 269
Console(config-ip-mask-acl)#mask host any 269
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#
```

Configuring an IP ACL Mask

This mask defines the fields to check in the IP header.

Command Usage

Masks that include an entry for a Layer 4 protocol source port or destination port can only be applied to packets with a header length of exactly five bytes**.**

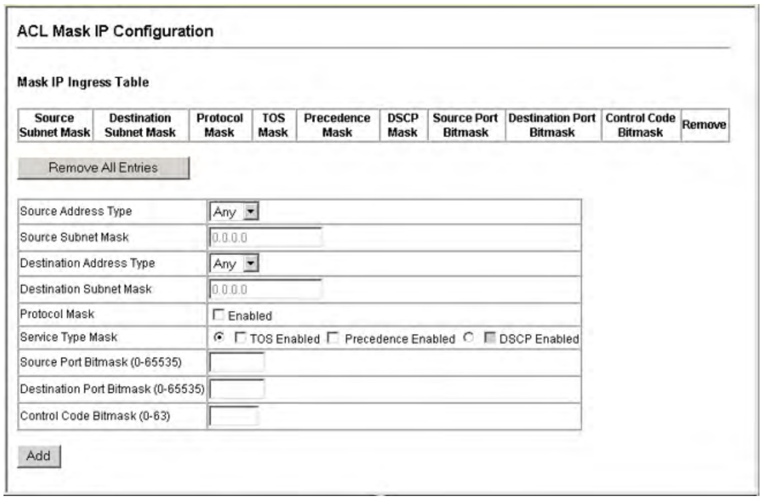
Command Attributes

Command Attributes	
• **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 Bitmask fields. • Options: Any, Host, MAC • Default: Any
• **Source/Destination Subnet Mask:**	Subnet mask for source or destination address. See the description for SubMask on page 74.
• **Protocol Bitmask:**	Check the protocol field.
• **Service Type Mask:**	Check the rule for the specified priority type. • Options: Precedence, TOS, DSCP • Default: TOS
• **Source/Destination Port Bitmask:**	Protocol port of rule must match this bitmask. • Range: 0-65535
• **Control Code Bitmask:**	Control flags of rule must match this bitmask. • Range: 0-63

Configuring an IP ACL Mask - Web

Configure the mask to match the required rules in the IP ingress or egress ACLs. Set the mask to check for any source or destination address, a specific host address, or an address range.

- Include other criteria to search for in the rules, such as a protocol type or one of the service types.
- Or use a bitmask to search for specific protocol port(s) or TCP control code(s). Then click **Add**.



ACL Mask IP Configuration

Mask IP Ingress Table

Source Subnet Mask	Destination Subnet Mask	Protocol Mask	TOS Mask	Precedence Mask	DSCP Mask	Source Port Bitmask	Destination Port Bitmask	Control Code Bitmask	Remove

Source Address Type	Any
Source Subnet Mask	0.0.0.0
Destination Address Type	Any
Destination Subnet Mask	0.0.0.0
Protocol Mask	□ Enabled
Service Type Mask	● □ TOS Enabled □ Precedence Enabled ○ □ DSCP Enabled
Source Port Bitmask (0-65535)	
Destination Port Bitmask (0-65535)	
Control Code Bitmask (0-63)	

FIG. 80 Web - Configuring an IP based ACL

Configuring an IP ACL Mask - CLI

This shows that the entries in the mask override the precedence in which the rules are entered into the ACL. In the following example, packets with the source address 10.1.1.1 are dropped because the “deny 10.1.1.1 255.255.255.255” rule has the higher precedence according the “**mask host any**” entry.

```
Console(config)#access-list ip standard A2                264
Console(config-std-acl)#permit 10.1.1.0 255.255.255.0     265
Console(config-std-acl)#deny 10.1.1.1 255.255.255.255
Console(config-std-acl)#exit
Console(config)#access-list ip mask-precedence in         269
Console(config-ip-mask-acl)#mask host any                 269
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#
```

Configuring a MAC ACL Mask

This mask defines the fields to check in the packet header.

Command Usage

You must configure a mask for an ACL rule before you can bind it to a port.

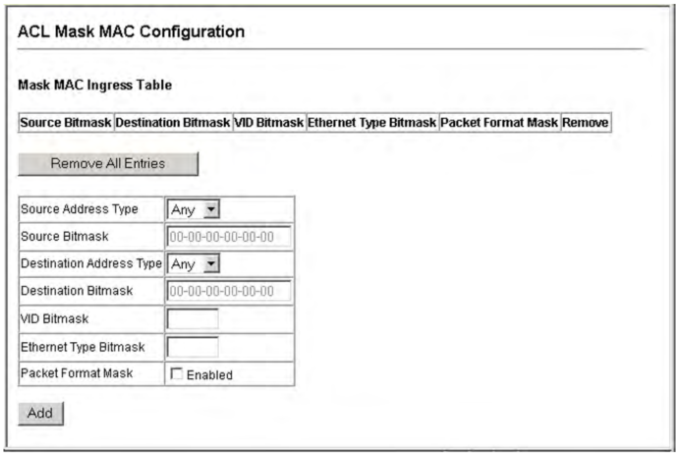
Command Attributes

Command Attributes	
• **Source/Destination Address Type:**	Use “Any” to match any address, “Host” to specify the host address for a single node, or “MAC” to specify a range of addresses. • Options: Any, Host, MAC • Default: Any
• **Source/Destination Bitmask:**	Address of rule must match this bitmask.
• **VID Bitmask:**	VLAN ID of rule must match this bitmask.
• **Ethernet Type Bitmask:**	Ethernet type of rule must match this bitmask.
• **Packet Format Mask:**	A packet format must be specified in the rule.

Configuring a MAC ACL Mask - Web

Configure the mask to match the required rules in the MAC ingress or egress ACLs. Set the mask to check for any source or destination address, a host address, or an address range.

Use a bitmask to search for specific VLAN ID(s) or Ethernet type(s). Or check for rules where a packet format was specified. Then click **Add**.



ACL Mask MAC Configuration

Mask MAC Ingress Table

Source Bitmask	Destination Bitmask	VID Bitmask	Ethernet Type Bitmask	Packet Format Mask	Remove

Remove All Entries

Source Address Type	Any
Source Bitmask	00-00-00-00-00-00
Destination Address Type	Any
Destination Bitmask	00-00-00-00-00-00
VID Bitmask	
Ethernet Type Bitmask	
Packet Format Mask	□ Enabled

Add

FIG. 81 Configuring a MAC based ACL

Configuring a MAC ACL Mask - CLI

This example shows how to create an Ingress MAC ACL and bind it to a port. You can then see that the order of the rules have been changed by the mask.

```
Console(config)#access-list mac M4
Console(config-mac-acl)#permit any any
Console(config-mac-acl)#denytagged-eth200-11-11-11-11-11ff-ff-ff-ff-ff-ffanyvid3
  278
Console(config-mac-acl)#end
Console#show access-list
MAC access-list M4:
  permit any any
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
Console(config)#access-list mac mask-precedence in
Console(config-mac-mask-acl)#mask pktformat ff-ff-ff-ff-ff-ff any vid
Console(config-mac-mask-acl)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#mac access-group M4 in
Console(config-if)#end
Console#show access-list
MAC access-list M4:
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
  permit any any
MAC ingress mask ACL:
  mask pktformat host any vid
Console#
```

Binding a Port to an Access Control List - Web

After configuring the Access Control Lists (ACL), you can bind the ports that need to filter traffic to the appropriate ACLs. You can only bind a port to one ACL for each basic type – *IP ingress*, *IP egress*, *MAC ingress* and *MAC egress*.

Command Usage

- This switch supports ACLs for both ingress and egress filtering. However, you can only bind one IP ACL and one MAC ACL to any port for ingress filtering, and one IP ACL and one MAC ACL to any port for egress filtering. In other words, only four ACLs can be bound to an interface – Ingress IP ACL, Egress IP ACL, Ingress MAC ACL and Egress MAC ACL.
- When an ACL is bound to an interface as an egress filter, all entries in the ACL must be deny rules. Otherwise, the bind operation will fail.

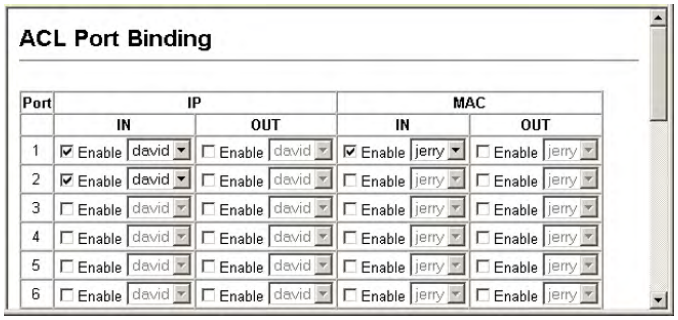
- The switch does not support the explicit “deny any” rule for the egress IP ACL or the egress MAC ACLs. If these rules are included in the ACL, and you attempt to bind the ACL to an interface for egress checking, the bind operation will fail.

Command Attributes

Command Attributes	
• **Port:**	Fixed port or SFP module. (Range: 1-24)
• **IP:**	Specifies the IP ACL to bind to a port.
• **MAC:**	Specifies the MAC ACL to bind to a port.
• **IN:**	ACL for ingress packets.
• **OUT:**	ACL for egress packets.
• ***ACL Name***:	Name of the ACL.

Binding a Port to an Access Control List - Web

Click *ACL*, *ACL Port Binding*. Mark the **Enable** field for the port you want to bind to an ACL for ingress or egress traffic, select the required ACL from the drop-down list, then click **Apply**.



ACL Port Binding

Port	IP		MAC	
	IN	OUT	IN	OUT
1	☑ Enable david	□ Enable david	☑ Enable jerry	□ Enable jerry
2	☑ Enable david	□ Enable david	□ Enable jerry	□ Enable jerry
3	□ Enable david	□ Enable david	□ Enable jerry	□ Enable jerry
4	□ Enable david	□ Enable david	□ Enable jerry	□ Enable jerry
5	□ Enable david	□ Enable david	□ Enable jerry	□ Enable jerry
6	□ Enable david	□ Enable david	□ Enable jerry	□ Enable jerry

FIG. 82 Mapping ACLs to Port Ingress/Egress Queues

Binding a Port to an Access Control List - CLI

This example assigns an IP and MAC ingress ACL to port 1, and an IP ingress ACL to port 2.

```
Console(config)#interface ethernet 1/1300
Console(config-if)#ip access-group david in273
Console(config-if)#mac access-group jerry in284
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#ip access-group david in
Console(config-if)#
```

Filtering IPs for Management Access

Overview

You can specify the client IP addresses that are allowed management access to the switch through the web interface, SNMP, or Telnet.

Command Usage

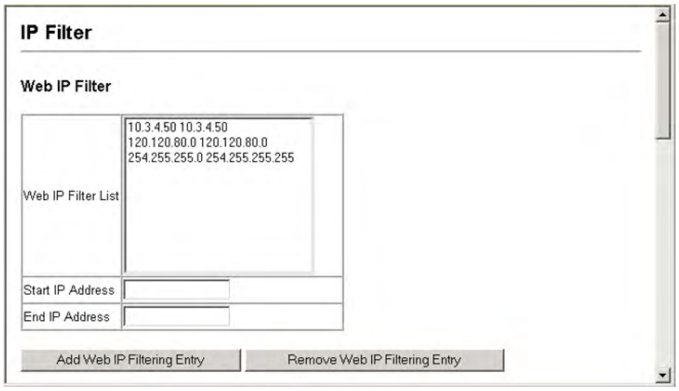
- The management interfaces are open to all IP addresses by default. Once you add an entry to a filter list, access to that interface is restricted to the specified addresses.
- If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- IP addresses 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.

Command Attributes

Command Attributes	
• **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.
• **IP Filter List:**	IP addresses that are allowed management access to this interface.
• **Start IP Address:**	A single IP address, or the starting address of a range.
• **End IP Address:**	The end address of a range.

Filtering IP Addresses for Management Access - Web

Click *Security*, *IP Filter*. Enter the addresses that are allowed management access to an interface, and click **Add IP Filtering Entry**.



IP Filter

Web IP Filter

Web IP Filter List	10.3.4.50 10.3.4.50
	120.120.80.0 120.120.80.0
	254.255.255.0 254.255.255.255

Start IP Address	
End IP Address	

FIG. 83 Entering IP Addresses to be Filtered

Filtering IP Addresses for Management Access - CLI

This example restricts management access for Telnet and SNMP clients.

```
Console(config)#management telnet-client 192.168.1.19                     198
Console(config)#management telnet-client 192.168.1.25 192.168.1.30
Console(config)#management snmp-client 10.1.2.3 255.255.255.255           198
Console(config)#end
Console#sh management telnet-client                                        199
Management IP Filter
 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#sh management snmp-client199
Management IP Filter
 SNMP-Client:
   Start IP address      End IP address
-----------------------------------------------
1. 10.1.2.3              255.255.255.255
Console#
```

Port Configuration

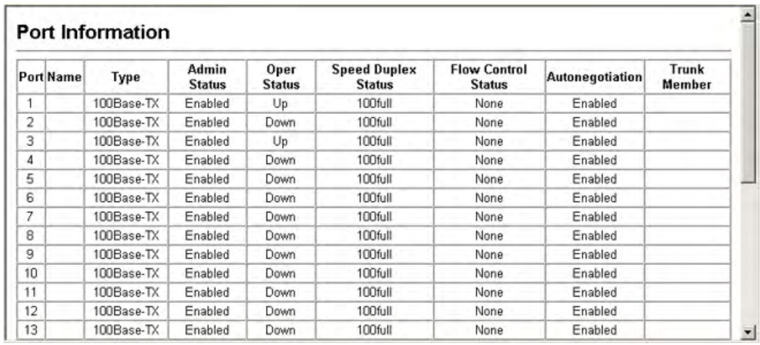
Overview

You can use the *Port Information* or *Trunk Information* pages to display the current connection status, including link state, speed/duplex mode, flow control, and auto-negotiation.

Field Attributes (Web)	
• **Name:**	Interface label.
• **Type:**	Indicates the port type (10BASE-T, 100BASE-TX, 100BASE-FX, 1000BASE-LX, 1000BASE-GBIC).
• **Admin Status:**	Shows if the interface is enabled or disabled.
• **Oper Status:**	Indicates if the link is Up or Down.
• **Speed Duplex Status:**	Shows the current speed and duplex mode. (Auto, or fixed choice)
• **Flow Control Status:**	Indicates the type of flow control currently in use. (IEEE 802.3x, Back-Pressure or None)
• **Autonegotiation:**	Shows if auto-negotiation is enabled or disabled.
• **Trunk Member:**	Shows if port is a trunk member. (Port Information only.)
• **Creation:**	Shows if a trunk is manually configured. (Trunk Information only.) or dynamically set via LACP.

Displaying Connection Status - Web

Click *Port*, *Port Information* or *Trunk Information*.



Port Information

Port	Name	Type	Admin Status	Oper Status	Speed Duplex Status	Flow Control Status	Autonegotiation	Trunk Member
1		100Base-TX	Enabled	Up	100full	None	Enabled	
2		100Base-TX	Enabled	Down	100full	None	Enabled	
3		100Base-TX	Enabled	Up	100full	None	Enabled	
4		100Base-TX	Enabled	Down	100full	None	Enabled	
5		100Base-TX	Enabled	Down	100full	None	Enabled	
6		100Base-TX	Enabled	Down	100full	None	Enabled	
7		100Base-TX	Enabled	Down	100full	None	Enabled	
8		100Base-TX	Enabled	Down	100full	None	Enabled	
9		100Base-TX	Enabled	Down	100full	None	Enabled	
10		100Base-TX	Enabled	Down	100full	None	Enabled	
11		100Base-TX	Enabled	Down	100full	None	Enabled	
12		100Base-TX	Enabled	Down	100full	None	Enabled	
13		100Base-TX	Enabled	Down	100full	None	Enabled	

FIG. 84 Web - Displaying Port/Trunk Information

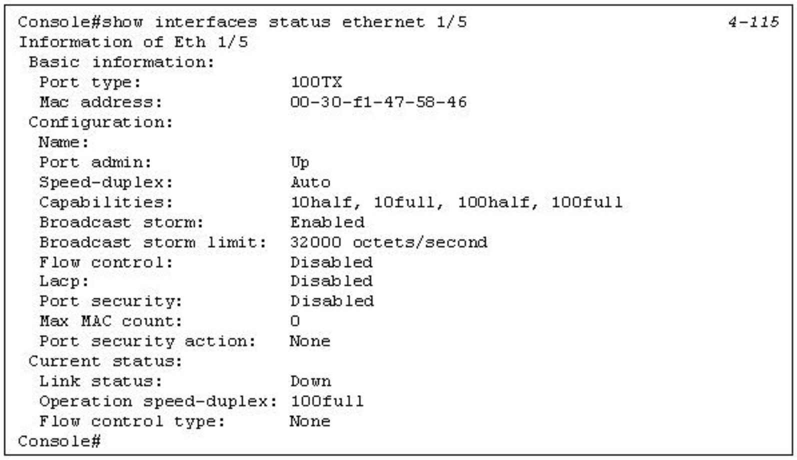
Field Attributes (CLI)

Field Attributes (CLI)	
Basic information:	
• **Port type:**	Indicates the port type. (10BASE-T, 100BASE-TX, 1000BASE-T, 1000BASE-SFP)
• **MAC address:**	The physical layer address for this port. To access this item on the web, see the *Setting an IP Address* section on page 13.
Configuration:	
• **Name:**	Interface label.
• **Port admin:**	Shows if the interface is enabled or disabled (i.e., up or down).
• **Speed-duplex:**	Shows the current speed and duplex mode. (Auto, or fixed choice)

Field Attributes (CLI - Cont.)	
• **Capabilities:**	Specifies the capabilities to be advertised for a port during auto-negotiation. To access this item on the web, see *Configuring Interface Connections* section on page 87. 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 - Supports 1000 Mbps full-duplex operation • Sym - Transmits and receives pause frames for flow control • FC - Supports flow control
• **Broadcast storm:**	Shows if broadcast storm control is enabled or disabled.
• **Broadcast storm limit:**	Shows the broadcast storm threshold. (500 - 262143 packets per second)
• **Flow control:**	Shows if flow control is enabled or disabled.
• **LACP:**	Shows if LACP is enabled or disabled.
• **Port Security:**	Shows if port security is enabled or disabled.
• **Max MAC count:**	Shows the maximum number of MAC address that can be learned by a port. (0 - 1024 addresses)
• **Port security action:**	Shows the response to take when a security violation is detected. (shutdown, trap, trap-and-shutdown)
Current status:	
• **Link Status:**	Indicates if the link is up or down.
• **Operation speed-duplex:**	Shows the current speed and duplex mode.
• **Flow control type:**	Indicates the type of flow control currently in use (IEEE 802.3x, Back-Pressure or none)

Displaying Connection Status - CLI

This example shows the connection status for Port 13.



```
Console#show interfaces status ethernet 1/5                          4-115
Information of Eth 1/5
 Basic information:
  Port type:               100TX
  Mac address:             00-30-f1-47-58-46
 Configuration:
  Name:
  Port admin:              Up
  Speed-duplex:            Auto
  Capabilities:            10half, 10full, 100half, 100full
  Broadcast storm:         Enabled
  Broadcast storm limit:   32000 octets/second
  Flow control:            Disabled
  Lacp:                    Disabled
  Port security:           Disabled
  Max MAC count:           0
  Port security action:    None
 Current status:
  Link status:             Down
  Operation speed-duplex:  100full
  Flow control type:       None
Console#
```

FIG. 85 CLI - Displaying Port/Trunk Information

Configuring Interface Connections

You can use the *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.

Command Attributes

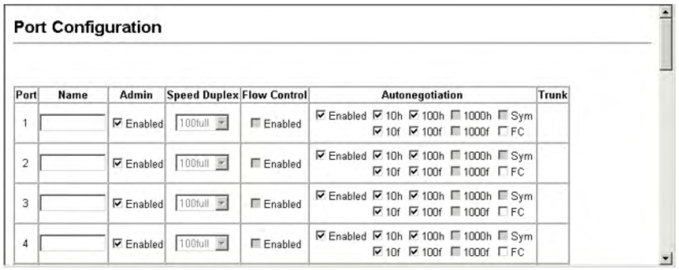
Command Attributes	
• **Name**	Allows you to label an interface. (Range: 1-64 characters)
• **Admin**	Allows you to manually disable an interface. You can disable an interface due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also disable an interface for security reasons.
• **Speed/Duplex**	Allows manual selection of port speed and duplex mode (i.e., with auto-negotiation disabled).
• **Flow Control**	Allows automatic or manual selection of flow control.
• **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 - Supports 1000 Mbps full-duplex operation • Sym (Gigabit only) - When specified, the port transmits and receives pause frames; when not specified, the port will auto-negotiate to determine the sender and receiver for asymmetric pause frames. (The current switch chip only supports symmetric pause frames.) • FC - Supports flow control 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 802.3x 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-LX – 1000full)
• **Trunk**	Indicates if a port is a member of a trunk. To create trunks and select port members, see *Creating Trunk Groups* section on page 88.

NOTE

Autonegotiation must be disabled before you can configure or force the interface to use the Speed/Duplex Mode or Flow Control options.

Configuring Interface Connections - Web

Click *Port*, *Port Configuration* or *Trunk Configuration*. Modify the required interface settings, and click **Apply**.



Port Configuration

Port	Name	Admin	Speed Duplex	Flow Control	Autonegotiation	Trunk
1		☑ Enabled	100full	□ Enabled	☑ Enabled ☑ 10h ☑ 100h □ 1000h □ Sym ☑ 10f ☑ 100f □ 1000f □ FC	
2		☑ Enabled	100full	□ Enabled	☑ Enabled ☑ 10h ☑ 100h □ 1000h □ Sym ☑ 10f ☑ 100f □ 1000f □ FC	
3		☑ Enabled	100full	□ Enabled	☑ Enabled ☑ 10h ☑ 100h □ 1000h □ Sym ☑ 10f ☑ 100f □ 1000f □ FC	
4		☑ Enabled	100full	□ Enabled	☑ Enabled ☑ 10h ☑ 100h □ 1000h □ Sym ☑ 10f ☑ 100f □ 1000f □ FC	

FIG. 86 Web - Port/Trunk Configuration

Configuring Interface Connections - CLI

Select the interface, and then enter the required settings.

```
Console(config)#interface ethernet 1/13                          4-108
Console(config-if)#description RD SW#13                          4-109
Console(config-if)#shutdown                                      4-113
.
Console(config-if)#no shutdown
Console(config-if)#no negotiation                                4-110
Console(config-if)#speed-duplex 100half                          4-109
Console(config-if)#flowcontrol                                   4-112
.
Console(config-if)#negotiation
Console(config-if)#capabilities 100half                          4-111
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
```

FIG. 87 CLI - Port/Trunk Configuration

Creating Trunk Groups

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 six trunks at a time.

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 four ports, all other ports will be placed in a 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 six trunks on the 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.

- 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.

Statically Configuring a Trunk

Command Usage

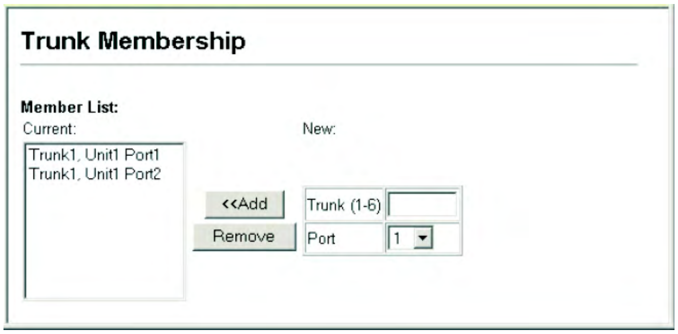
- When configuring static trunks, you may not be able to link switches of different types, depending on the manufacturer's implementation. However, note that the static trunks on this switch are Cisco EtherChannel compatible.
- To avoid creating a loop in the network, be sure you add a static trunk via the configuration interface before connecting the ports, and also disconnect the ports before removing a static trunk via the configuration interface.

Command Attributes

Command Attributes	
• **Member List (Current):**	Shows configured trunks (Trunk ID, Unit, Port).
• **New:**	Includes entry fields for creating new trunks.
• **Trunk:**	Trunk identifier. (Range: 1-4)
• **Unit:**	Stack unit. (Range: 1-8)
• **Port:**	Port identifier. (Range: 1-26)

Statically Configuring a Trunk - Web

Click *Port*, *Trunk Membership*. Enter a trunk ID of 1-6 in the *Trunk* field, select any of the switch ports from the scroll-down port list, and click **Add**. After you have completed adding ports to the member list, click **Apply**.


Trunk Membership

Member List:

Current:

Trunk1, Unit1 Port1
Trunk1, Unit1 Port2

New:

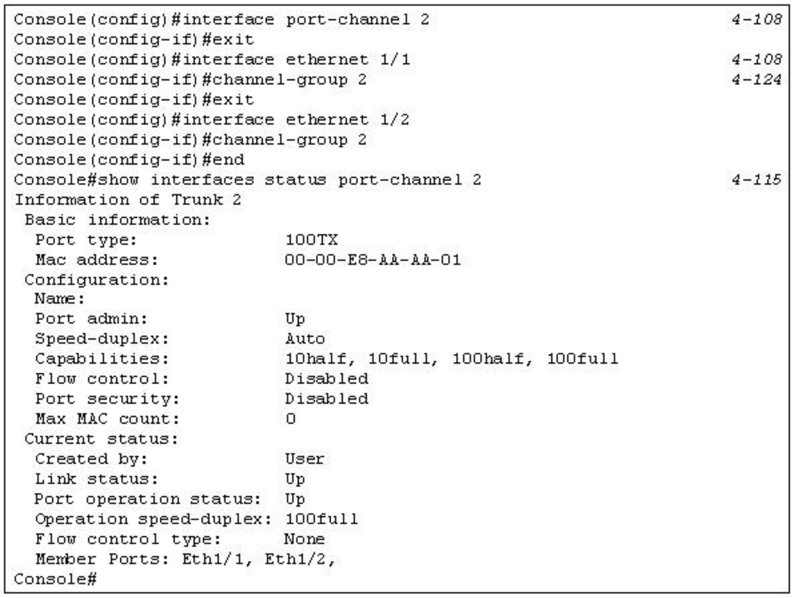
Trunk (1-6)

Port: 1

FIG. 88 Web - Configuring Port Trunks

Statically Configuring a Trunk - CLI

This example creates trunk 2 with ports 1 and 2. Just connect these ports to two static trunk ports on another switch to form a trunk.



```
Console(config)#interface port-channel 2                          4-108
Console(config-if)#exit
Console(config)#interface ethernet 1/1                            4-108
Console(config-if)#channel-group 2                                4-124
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#channel-group 2
Console(config-if)#end
Console#show interfaces status port-channel 2                     4-115
Information of Trunk 2
 Basic information:
  Port type:                100TX
  Mac address:              00-00-E8-AA-AA-01
 Configuration:
  Name:
  Port admin:               Up
  Speed-duplex:             Auto
  Capabilities:             10half, 10full, 100half, 100full
  Flow control:             Disabled
  Port security:            Disabled
  Max MAC count:            0
 Current status:
  Created by:               User
  Link status:              Up
  Port operation status:    Up
  Operation speed-duplex:   100full
  Flow control type:        None
  Member Ports: Eth1/1, Eth1/2,
Console#
```

FIG. 89 CLI - Configuring Port Trunks

Enabling LACP on Selected Ports

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 four 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, either by forced mode or auto-negotiation.

Command Attributes

Command Attributes	
• **Member List (Current):**	Shows configured trunks (Unit, Port).
• **New:**	Includes entry fields for creating new trunks. • **Unit** – Stack unit. (Range: 1-8) • **Port** – Port identifier. (Range: 1-26)

Enabling LACP on Selected Ports - Web

Click *Port*, *LACP*, *Configuration*. Select any of the switch ports from the scroll-down port list and click Add. After you have completed adding ports to the member list, click **Apply**.

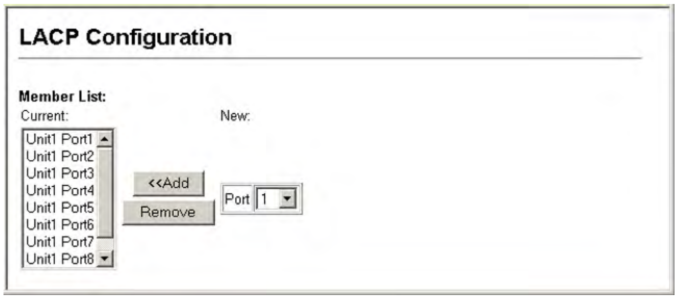
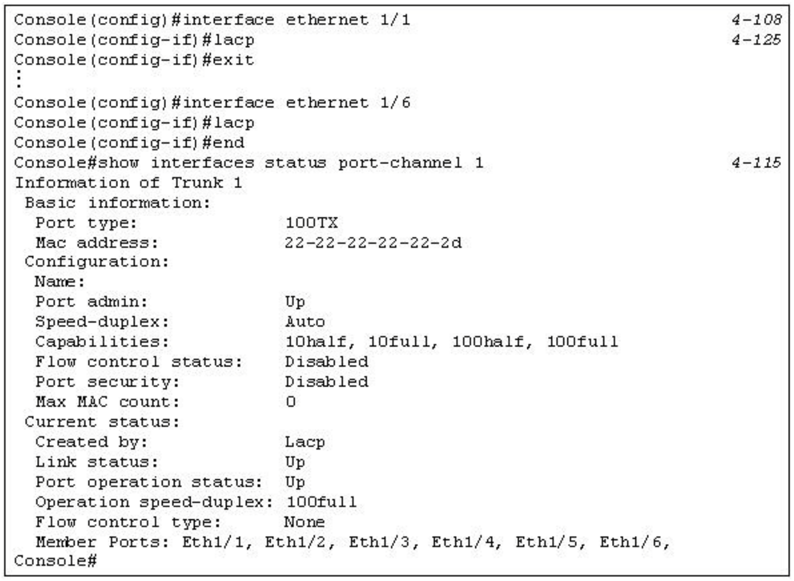


FIG. 90 Web - LACP Configuration

Enabling LACP on Selected Ports - CLI

The following example enables LACP for ports 1 to 6. Just connect these ports to LACP-enabled trunk ports on another switch to form a trunk.



```
Console(config)#interface ethernet 1/1                               4-108
Console(config-if)#lacp                                              4-125
Console(config-if)#exit
 :
Console(config)#interface ethernet 1/6
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 1                        4-115
Information of Trunk 1
 Basic information:
  Port type:                100TX
  Mac address:              22-22-22-22-22-2d
 Configuration:
  Name:
  Port admin:               Up
  Speed-duplex:             Auto
  Capabilities:             10half, 10full, 100half, 100full
  Flow control status:      Disabled
  Port security:            Disabled
  Max MAC count:            0
 Current status:
  Created by:               Lacp
  Link status:              Up
  Port operation status:    Up
  Operation speed-duplex:   100full
  Flow control type:        None
  Member Ports: Eth1/1, Eth1/2, Eth1/3, Eth1/4, Eth1/5, Eth1/6,
Console#
```

FIG. 91 CLI - LACP Configuration

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.
- However, if the "port channel" Admin Key is set (page 318), then the port Admin Key must be set to the same value for a port to be allowed to join a channel group.

NOTE

If the port channel admin key (LACP admin key, page 318) is not set (through the CLI) when a channel group is formed (i.e., it has a null value of 0), this key is set to the same value as the port admin key used by the interfaces that joined the group (LACP admin key, as described in this section and on page 318).

- **Set Port Actor** – This menu sets the local side of an aggregate link; i.e., the ports on this switch.
- **Set Port Partner** – This menu 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. However, 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.

Command Attributes

Command Attributes	
• **Port:**	Port number. (Range: 1-24)
• **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: 0
• **Port Priority:**	If a link goes down, LACP port priority is used to select a backup link. • Range: 0-65535 • Default: 32768

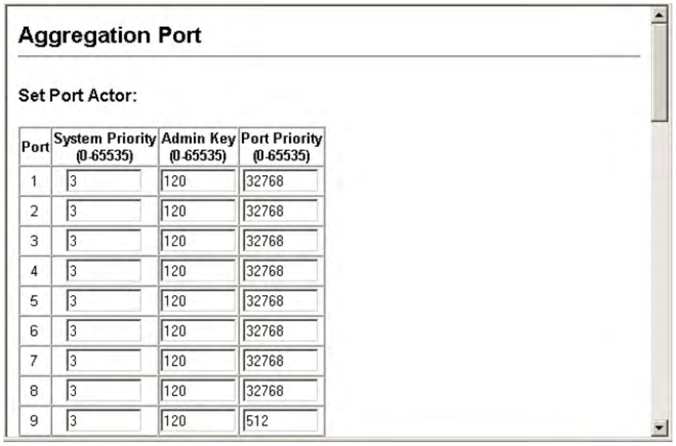
Dynamically Creating a Port Channel - Web

Click *Port*, *LACP*, *Aggregation Port*. Set the System Priority, Admin Key, and Port Priority for the Port Actor. You can optionally configure these settings for the Port Partner.

NOTE

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.

After you have completed setting the port LACP parameters, click **Apply**.



Aggregation Port

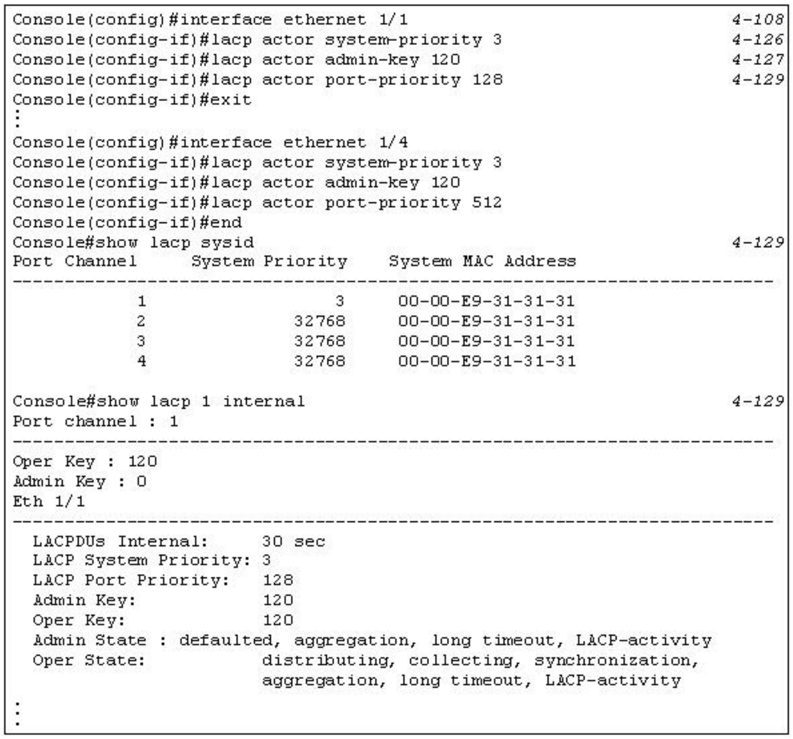
Set Port Actor:

Port	System Priority (0-65535)	Admin Key (0-65535)	Port Priority (0-65535)
1	3	120	32768
2	3	120	32768
3	3	120	32768
4	3	120	32768
5	3	120	32768
6	3	120	32768
7	3	120	32768
8	3	120	32768
9	3	120	512

FIG. 92 Web - LACP Port Configuration

Dynamically Creating a Port Channel - CLI

The following example configures LACP parameters for ports 1-6. Ports 1-4 are used as active members of the LAG; ports 5 and 6 are set to backup mode.



```
Console(config)#interface ethernet 1/1                                  4-108
Console(config-if)#lacp actor system-priority 3                         4-126
Console(config-if)#lacp actor admin-key 120                             4-127
Console(config-if)#lacp actor port-priority 128                         4-129
Console(config-if)#exit
:
Console(config)#interface ethernet 1/4
Console(config-if)#lacp actor system-priority 3
Console(config-if)#lacp actor admin-key 120
Console(config-if)#lacp actor port-priority 512
Console(config-if)#end
Console#show lacp sysid                                                 4-129
Port Channel     System Priority    System MAC Address
-------------------------------------------------------------------------
            1                  3      00-00-E9-31-31-31
            2              32768      00-00-E9-31-31-31
            3              32768      00-00-E9-31-31-31
            4              32768      00-00-E9-31-31-31

Console#show lacp 1 internal                                            4-129
Port channel : 1
-------------------------------------------------------------------------
Oper Key : 120
Admin Key : 0
Eth 1/1
-------------------------------------------------------------------------
  LACPDUs Internal:      30 sec
  LACP System Priority: 3
  LACP Port Priority:    128
  Admin Key:             120
  Oper Key:              120
  Admin State : defaulted, aggregation, long timeout, LACP-activity
  Oper State:            distributing, collecting, synchronization,
                         aggregation, long timeout, LACP-activity
:
```

FIG. 93 Web - LACP Port Configuration

Displaying LACP Port Counters

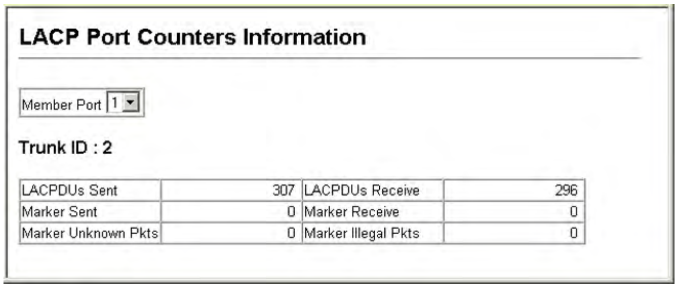
You can display statistics for LACP protocol messages. The following table describes the *Counter Information* fields:

Counter Information Fields

Counter Information Fields	
• **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.

Displaying LACP Port Counters - Web

Click *Port*, *LACP*, *Port Counters Information*. Select a member port to display the corresponding information.



LACP Port Counters Information

Member Port 1

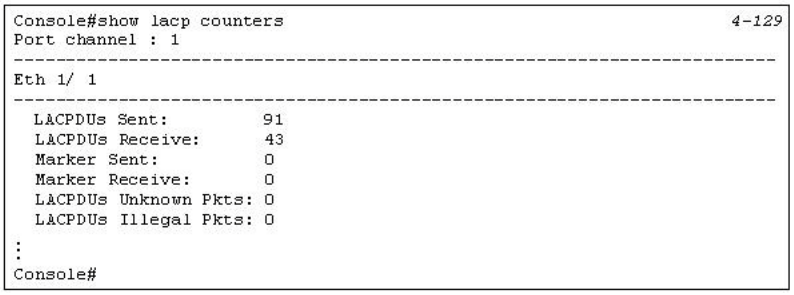
Trunk ID : 2

LACPDUs Sent	307	LACPDUs Receive	296
Marker Sent	0	Marker Receive	0
Marker Unknown Pkts	0	Marker Illegal Pkts	0

FIG. 94 Web - Displaying LACP Port Counters

Displaying LACP Port Counters - CLI

The following example displays LACP counters for port channel 1.



```
Console#show lacp counters                                           4-129
Port channel : 1
--------------------------------------------------------------------------
Eth 1/ 1
--------------------------------------------------------------------------
  LACPDUs Sent:         91
  LACPDUs Receive:      43
  Marker Sent:          0
  Marker Receive:       0
  LACPDUs Unknown Pkts: 0
  LACPDUs Illegal Pkts: 0
:
Console#
```

FIG. 95 CLI - Displaying LACP Port Counters

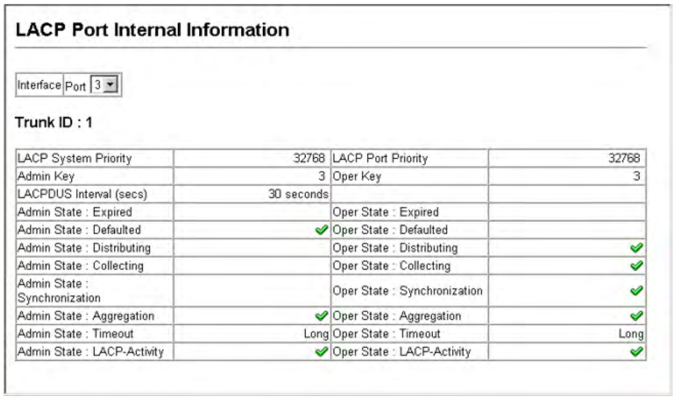
Displaying LACP Settings and Status for the Local Side

You can display configuration settings and the operational state for the local side of an link aggregation.

Displaying LACP Local Settings	
• **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.
• **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)

Displaying LACP Settings and Status for the Local Side - Web

Click *Port*, *LACP*, *Port Internal Information*. Select a port channel to display the corresponding information.



LACP Port Internal Information

Interface Port 3

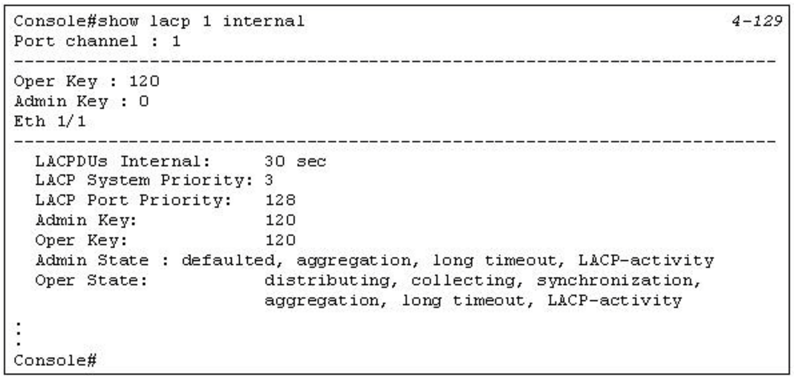
Trunk ID : 1

LACP System Priority	32768	LACP Port Priority	32768
Admin Key	3	Oper Key	3
LACPDUS Interval (secs)	30 seconds		
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	✓

FIG. 96 Web - Displaying LACP Port Information

Displaying LACP Settings and Status for the Local Side - CLI

The following example displays the LACP configuration settings and operational state for the local side of port channel 1.



```
Console#show lacp 1 internal                                          4-129
Port channel : 1
-------------------------------------------------------------------------
Oper Key : 120
Admin Key : 0
Eth 1/1
-------------------------------------------------------------------------
  LACPDUs Internal:      30 sec
  LACP System Priority: 3
  LACP Port Priority:    128
  Admin Key:             120
  Oper Key:              120
  Admin State : defaulted, aggregation, long timeout, LACP-activity
  Oper State:            distributing, collecting, synchronization,
                         aggregation, long timeout, LACP-activity
:
:
Console#
```

FIG. 97 CLI - Displaying LACP Port Information

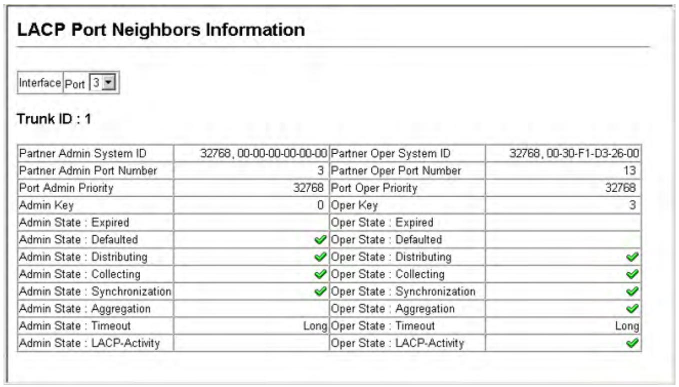
Displaying LACP Settings and Status for the Remote Side

You can display configuration settings and the operational state for the remote side of an link aggregation.

Displaying LACP Remote Settings - Neighbor Configuration Information	
• **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.)

Displaying LACP Settings and Status for the Remote Side - Web

Click Port, LACP, Port Neighbors Information. Select a port channel to display the corresponding information.



LACP Port Neighbors Information

Interface Port 3

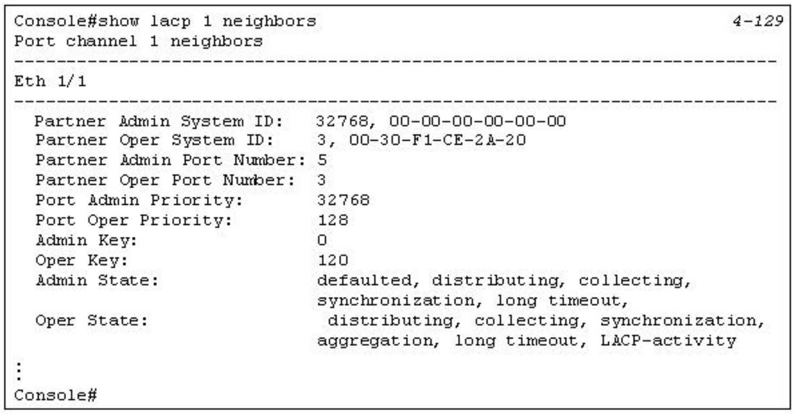
Trunk ID : 1

Partner Admin System ID	32768, 00-00-00-00-00-00	Partner Oper System ID	32768, 00-30-F1-D3-26-00
Partner Admin Port Number	3	Partner Oper Port Number	13
Port Admin Priority	32768	Port Oper Priority	32768
Admin Key	0	Oper Key	3
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	✓

FIG. 98 Web - Displaying Remote LACP Port Information

Displaying LACP Settings and Status for the Remote Side - CLI

The following example displays the LACP configuration settings and operational state for the remote side of port channel 1.



```
Console#show lacp 1 neighbors                                           4-129
Port channel 1 neighbors
-------------------------------------------------------------------------
Eth 1/1
-------------------------------------------------------------------------
  Partner Admin System ID:    32768, 00-00-00-00-00-00
  Partner Oper System ID:     3, 00-30-F1-CE-2A-20
  Partner Admin Port Number:  5
  Partner Oper Port Number:   3
  Port Admin Priority:        32768
  Port Oper Priority:         128
  Admin Key:                  0
  Oper Key:                   120
  Admin State:                defaulted, distributing, collecting,
                              synchronization, long timeout,
  Oper State:                  distributing, collecting, synchronization,
                              aggregation, long timeout, LACP-activity
:
Console#
```

FIG. 99 CLI - Displaying Remote LACP Port Information

Setting Broadcast Storm 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 for all ports. Any broadcast packets exceeding the specified threshold will then be dropped.

Command Usage

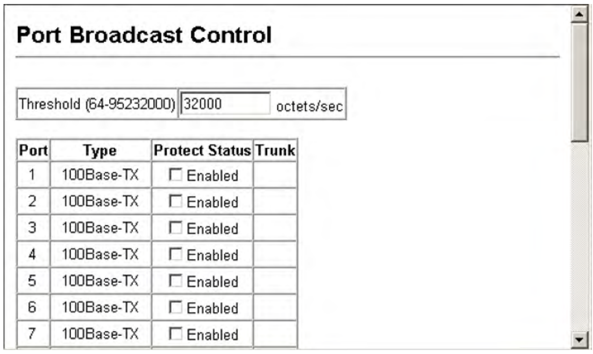
- Broadcast Storm Control is enabled by default.
- The default threshold is 500 packets per second.
- Broadcast control does not effect IP multicast traffic.
- The specified threshold applies to all ports on the switch.

Command Attributes

Command Attributes	
• **Threshold:**	Threshold as percentage of port bandwidth. • Options: 500-262143 packets per second • Default: 500 packets per second
• **Broadcast Control Status:**	Shows whether or not broadcast storm control has been enabled. • Default: Enabled

Setting Broadcast Storm Thresholds - Web

Click *Port*, *Broadcast Control*. Set the threshold any port, click **Apply**.



Port Broadcast Control

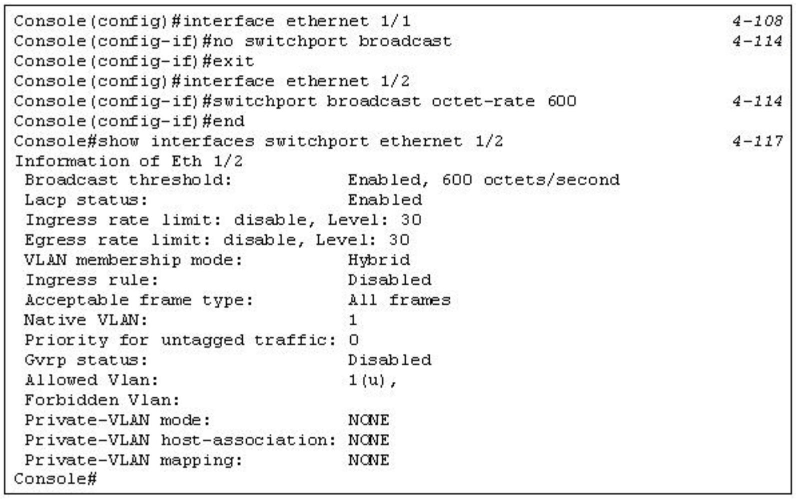
Threshold (64-95232000) 32000 octets/sec

Port	Type	Protect Status	Trunk
1	100Base-TX	□ Enabled	
2	100Base-TX	□ Enabled	
3	100Base-TX	□ Enabled	
4	100Base-TX	□ Enabled	
5	100Base-TX	□ Enabled	
6	100Base-TX	□ Enabled	
7	100Base-TX	□ Enabled	

FIG. 100 Web - Enabling Port Broadcast Control

Setting Broadcast Storm Thresholds - CLI

Specify any interface, and then enter the threshold. The following disables broadcast storm control for port 1, and then sets broadcast suppression at 600 packets per second for port 2.



```
Console(config)#interface ethernet 1/1                                 4-108
Console(config-if)#no switchport broadcast                             4-114
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#switchport broadcast octet-rate 600                 4-114
Console(config-if)#end
Console#show interfaces switchport ethernet 1/2                        4-117
Information of Eth 1/2
 Broadcast threshold:           Enabled, 600 octets/second
 Lacp status:                   Enabled
 Ingress rate limit: disable, Level: 30
 Egress rate limit: disable, Level: 30
 VLAN membership mode:          Hybrid
 Ingress rule:                  Disabled
 Acceptable frame type:         All frames
 Native VLAN:                   1
 Priority for untagged traffic: 0
 Gvrp status:                   Disabled
 Allowed Vlan:                  1(u),
 Forbidden Vlan:
 Private-VLAN mode:             NONE
 Private-VLAN host-association: NONE
 Private-VLAN mapping:          NONE
Console#
```

FIG. 101 CLI - Enabling Port Broadcast Control

Configuring Port Mirroring

You can 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.

Command Usage

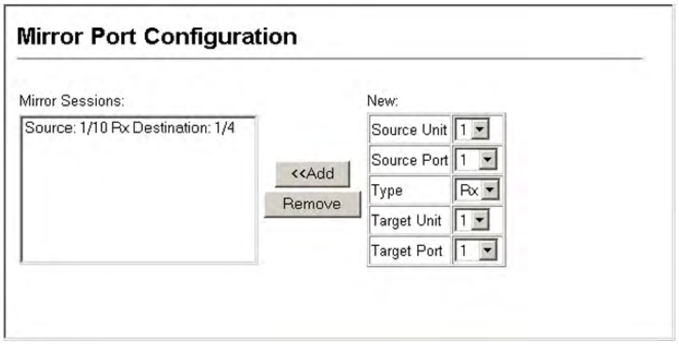
- Monitor port speed should match or exceed source port speed, otherwise traffic may be dropped from the monitor port.
- All mirror sessions have to share the same destination port.
- When mirroring port traffic, the target port must be included in the same VLAN as the source port.

Command Attributes

Command Attributes	
• **Mirror Sessions:**	Displays a list of current mirror sessions.
• **Source Unit:**	The unit whose port traffic will be monitored.
• **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.
• **Target Unit:**	The unit whose port will “duplicate” or “mirror” the traffic on the source port.
• **Target Port:**	The port that will “duplicate” or “mirror” the traffic on the source port.

Configuring Port Mirroring - Web

Click Port, Mirror Port Configuration. Specify the source port/unit, the traffic type to be mirrored, and the monitor port/unit, then click **Add**.



Mirror Port Configuration

Mirror Sessions:
Source: 1/10 Rx Destination: 1/4

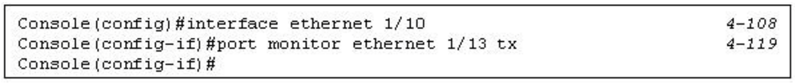
New:

Source Unit	1
Source Port	1
Type	Rx
Target Unit	1
Target Port	1

FIG. 102 Web - Mirror Port Configuration

Configuring Port Mirroring - CLI

Use the interface command to select the monitor port, then use the port monitor command to specify the source port. Note that default mirroring under the CLI is for both received and transmitted packets.



```
Console(config)#interface ethernet 1/10                              4-108
Console(config-if)#port monitor ethernet 1/13 tx                     4-119
Console(config-if)#
```

FIG. 103 Web - Mirror Port Configuration

Configuring Rate Limits

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 coming out of the switch. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

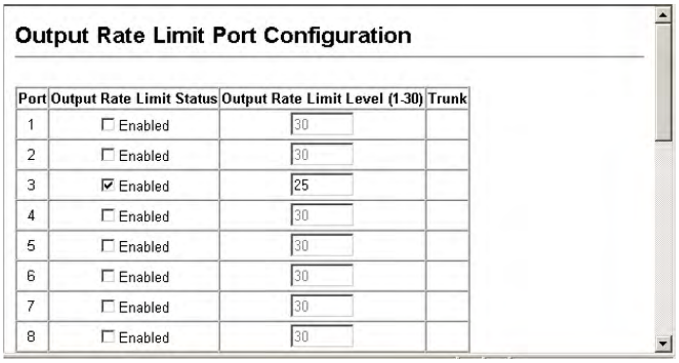
Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

Command Attributes

Command Attributes	
• **Rate Limit:**	Sets the output rate limit for an interface. • Default Status – Disabled • Default Rate – 100 Mbps • Range – 1 - 1000 Mbps

Configuring Rate Limits - Web

Click *Rate Limit*, *Input/Output Port/Trunk Configuration*. Set the *Input Rate Limit Status* or *Output Rate Limit Status*, then set the rate limit for the individual interfaces, and click **Apply**.



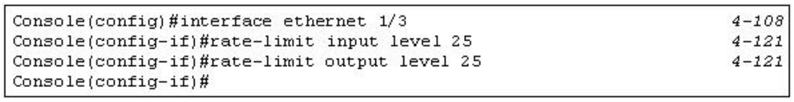
Output Rate Limit Port Configuration

Port	Output Rate Limit Status	Output Rate Limit Level (1-30)	Trunk
1	☐ Enabled	30	
2	☐ Enabled	30	
3	☑ Enabled	25	
4	☐ Enabled	30	
5	☐ Enabled	30	
6	☐ Enabled	30	
7	☐ Enabled	30	
8	☐ Enabled	30	

FIG. 104 Web - Output Rate Limit Port Configuration

Configuring Rate Limits - CLI

This example sets the rate limit for input and output traffic passing through port 3 to 600 Mbps.



```
Console(config)#interface ethernet 1/3                                  4-108
Console(config-if)#rate-limit input level 25                            4-121
Console(config-if)#rate-limit output level 25                           4-121
Console(config-if)#
```

FIG. 105 CLI - Output Rate Limit Port Configuration

Showing Port Statistics

You can 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.

RMON groups 2, 3 and 9 can only be accessed using SNMP management software such as HP OpenView.

Port Statistics

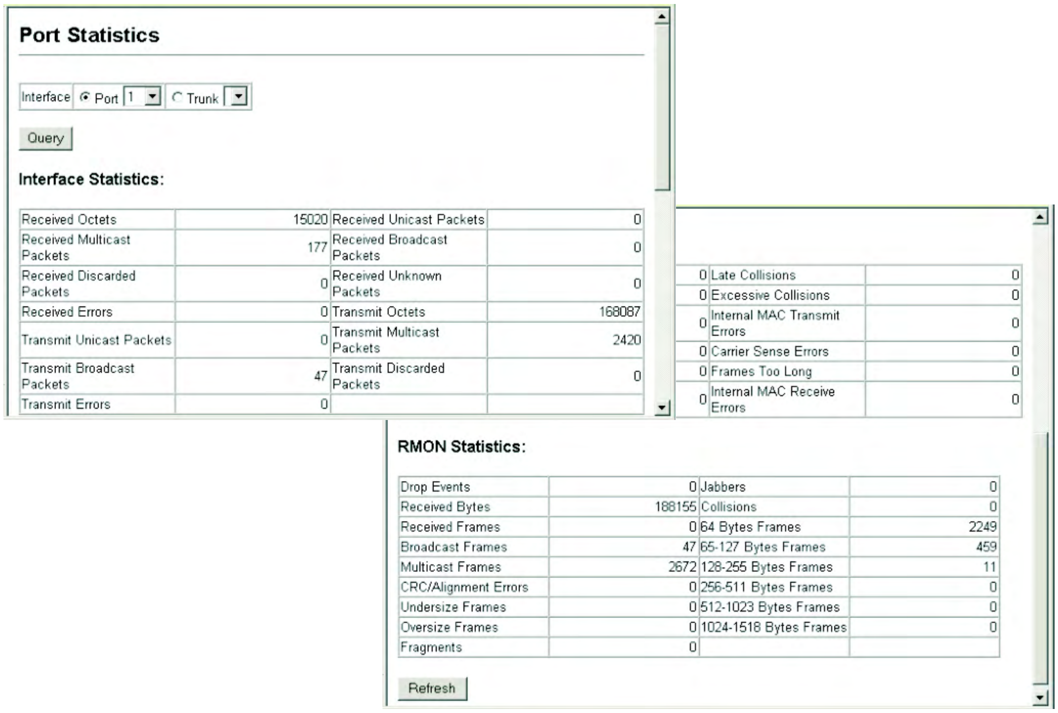
Port Statistics	
Interface Statistics	
• **Received Octets:**	The total number of octets received on the interface, including framing characters.
• **Received Unicast Packets:**	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
• **Received Multicast Packets:**	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
• **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.
• **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.
• **Received Unknown Packets:**	The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.
• **Received Errors:**	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

Port Statistics (Cont.)	
Interface Statistics (Cont.)	
• **Transmit Octets:**	The total number of octets transmitted out of the interface, including framing characters.
• **Transmit 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.
• **Transmit 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.
• **Transmit 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.
• **Transmit 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.
• **Transmit Errors:**	The number of outbound packets that could not be transmitted because of errors.
Etherlike Statistics	
• **Alignment Errors:**	The number of alignment errors (missynchronized data packets).
• **Late Collisions:**	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
• **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.
• **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.
• **Single Collision Frames:**	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
• **Internal MAC Transmit Errors:**	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.
• **Multiple Collision Frames:**	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
• **Carrier Sense Errors:**	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
• **SQE Test Errors:**	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface.
• **Frames Too Long:**	A count of frames received on a particular interface that exceed the maximum permitted frame size.
• **Deferred Transmissions:**	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
• **Internal MAC Receive Errors:**	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive 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.
• **Received Bytes:**	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.

Port Statistics (Cont.)	
RMON Statistics (Cont.)	
• **Collisions:**	The best estimate of the total number of collisions on this Ethernet segment.
• **Received Frames:**	The total number of frames (bad, broadcast and multicast) received.
• **Broadcast Frames:**	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
• **Multicast Frames:**	The total number of good frames received that were directed to this multicast address.
• **CRC/Alignment Errors:**	The number of CRC/alignment errors (FCS or alignment errors).
• **Undersize Frames:**	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
• **Oversize Frames:**	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
• **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.
• **64 Bytes Frames:**	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
• **65-127 Byte Frames:** • **128-255 Byte Frames:** • **256-511 Byte Frames:** • **512-1023 Byte Frames:** • **1024-1518 Byte Frames:** • **1519-1536 Byte Frames:**	The total number of frames (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).

Showing Port Statistics - Web

Click *Port*, *Port Statistics*. Select the required interface, and click **Query**. You can also use the **Refresh** button at the bottom of the page to update the screen.



Port Statistics

Interface ● Port 1 ○ Trunk

Interface Statistics:

Received Octets	15020	Received Unicast Packets	0
Received Multicast Packets	177	Received Broadcast Packets	0
Received Discarded Packets	0	Received Unknown Packets	0
Received Errors	0	Transmit Octets	168087
Transmit Unicast Packets	0	Transmit Multicast Packets	2420
Transmit Broadcast Packets	47	Transmit Discarded Packets	0
Transmit Errors	0		

0	Late Collisions	0
0	Excessive Collisions	0
0	Internal MAC Transmit Errors	0
0	Carrier Sense Errors	0
0	Frames Too Long	0
0	Internal MAC Receive Errors	0

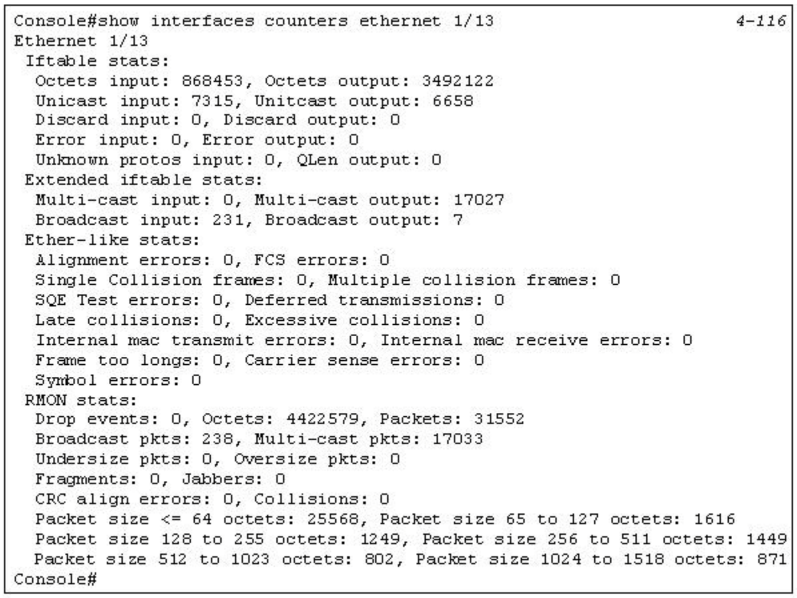
RMON Statistics:

Drop Events	0	Jabbers	0
Received Bytes	188155	Collisions	0
Received Frames	0	64 Bytes Frames	2249
Broadcast Frames	47	65-127 Bytes Frames	459
Multicast Frames	2672	128-255 Bytes Frames	11
CRC/Alignment Errors	0	256-511 Bytes Frames	0
Undersize Frames	0	512-1023 Bytes Frames	0
Oversize Frames	0	1024-1518 Bytes Frames	0
Fragments	0		

FIG. 106 Web - Displaying Port Statistics

Showing Port Statistics - CLI

This example shows statistics for port 13.



```
Console#show interfaces counters ethernet 1/13                           4-116
Ethernet 1/13
 Iftable stats:
  Octets input: 868453, Octets output: 3492122
  Unicast input: 7315, Unitcast output: 6658
  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: 0, Multi-cast output: 17027
  Broadcast input: 231, Broadcast output: 7
 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
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
 RMON stats:
  Drop events: 0, Octets: 4422579, Packets: 31552
  Broadcast pkts: 238, Multi-cast pkts: 17033
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 25568, Packet size 65 to 127 octets: 1616
  Packet size 128 to 255 octets: 1249, Packet size 256 to 511 octets: 1449
  Packet size 512 to 1023 octets: 802, Packet size 1024 to 1518 octets: 871
Console#
```

FIG. 107 CLI - Displaying Port Statistics

Power Over Ethernet (PoE) Settings

Overview

This switch can provide DC power to a wide range of connected devices, eliminating the need for an additional power source and cutting down on the amount of cables attached to each device. Once configured to supply power, an automatic detection process is initialized by the switch that is authenticated by a PoE signature from the connected device. Detection and authentication prevent damage to non-802.3af compliant devices.

The switch's power management enables total switch power and individual port power to be controlled within a configured power budget. Port power can be automatically turned on and off for connected devices, and a per-port power priority can be set so that the switch never exceeds its allocated power budget. When a device is connected to a switch port, its power requirements are detected by the switch before power is supplied. If the power required by a device exceeds the power budget of the port or the whole switch, power is not supplied.

Ports can be set to one of three power priority levels, critical, high, or low. To control the power supply within the switch's budget, ports set at critical or high priority have power enabled in preference to those ports set at low priority. For example, when a device is connected to a port set to critical priority, the switch supplies the required power, if necessary by dropping power to ports set for a lower priority. If power is dropped to some low-priority ports and later the power demands on the switch fall back within its budget, the dropped power is automatically restored.

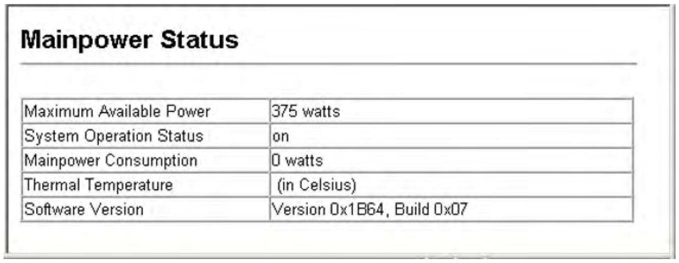
Switch Power Status

Displays the current status of power parameters for the switch.

Command Attributes	
• Maximum Available Power:	The current configured power budget for the switch. (Default 375 watts)
• System Operation Status:	The current operating PoE power status for the switch.
• Mainpower Consumption:	The current amount of power being consumed by PoE devices connected to the switch.
• Thermal Temperature:	The current internal temperature of the switch.
• Software Version:	The version of software running on the PoE controller subsystem in the switch.

Switch Power Status - Web

Click PoE, then Power Status.



Mainpower Status

Maximum Available Power	375 watts
System Operation Status	on
Mainpower Consumption	0 watts
Thermal Temperature	(in Celsius)
Software Version	Version 0x1B64, Build 0x07

FIG. 108 Displaying the Global PoE Status

Switch Power Status - CLI

This example displays the current power status for the switch.

```
Console#show power mainpower243
Unit 1 Mainpower Status
 Maximum Available Power : 375 watts
 System Operation Status : on
 Mainpower Consumption   : 0 watts
 Software Version        : Version 0x1B64, Build 0x07
Console#
```

Setting a Switch Power Budget

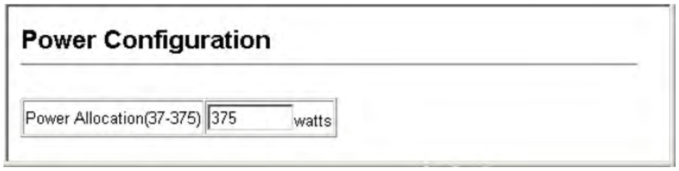
A maximum PoE power budget for the switch (power available to all switch ports) can be defined so that power can be centrally managed, preventing overload conditions at the power source.

If the power demand from devices connected to the switch exceeds the power budget setting, the switch uses port power priority settings to limit the supplied power.

Command Attributes	
• **Power Allocation:**	The power budget for the switch. If devices connected to the switch require more power than the switch budget, the port power priority settings are used to control the supplied power. • Range: 37 - 375 watts • Default:375 Watts

Setting a Switch Power Budget - Web

Click PoE, Power Config. Specify the desired power budget for the switch. Click **Apply**.



Power Configuration

Power Allocation(37-375) 375 watts

FIG. 109 Web - Power Configuration

Setting a Switch Power Budget - CLI

CLI – Use the **power mainpower maximum allocation** command to set the PoE power budget for the switch.

```
Console(config)#power mainpower maximum allocation 200
```

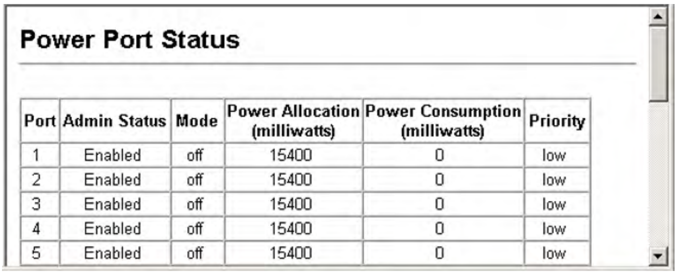
Displaying Port Power Status

Use the Power Port Status page to display the current PoE power status for all ports.

Command Attributes	
• **Port:**	The port number.
• **Admin Status:**	The administrative status of PoE power on the port. • Default: Enabled
• **Mode:**	The current operating status of PoE power on the port. (On or off.)
• **Power Allocation:**	The configured power budget for the port. • Range: 3000-15400 milliwatts • Default: 15400 milliwatts
• **Power Consumption:**	The current power consumption on the port.
• **Priority:**	The port's configured power priority setting. • Options: Low, High, or Critical • Default: Low

Displaying Port Power Status - Web

Click PoE, followed by Power Port Status.



Power Port Status

Port	Admin Status	Mode	Power Allocation (milliwatts)	Power Consumption (milliwatts)	Priority
1	Enabled	off	15400	0	low
2	Enabled	off	15400	0	low
3	Enabled	off	15400	0	low
4	Enabled	off	15400	0	low
5	Enabled	off	15400	0	low

FIG. 110 Web - Power Port Status

Displaying Port Power Status - CLI

This example displays the PoE status and the priority of port 1.

```
Console#show power inline status                                      242
Interface  Admin   Oper Power(mWatt) Power(used)  Priority
---------- ------- ---- ------------ ------------ --------
Eth   1/ 1  enable  off        15400            0       low
Eth   1/ 2  enable  off        15400            0       low
Eth   1/ 3  enable   on        15400         7505       low
Eth   1/ 4  enable  off        15400            0       low
Eth   1/ 5  enable  off        15400            0       low
Eth   1/ 6  enable  off        15400            0       low
Eth   1/ 7  enable   on        15400         8597       low
.
.
.
Eth   1/23  enable  off        15400            0       low
Eth   1/24  enable  off        15400            0       low
Console#
```

Configuring Port PoE Power

If a device is connected to a switch port and the switch detects that it requires more than the power budget of the port, no power is supplied to the device (the port power remains off).

NOTE

Power is dropped from low-priority ports in sequence starting from port number 1.

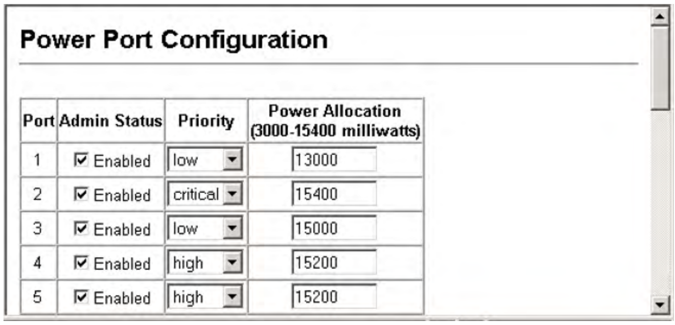
If the power demand from devices connected to switch ports exceeds the power budget set for the switch, the port power priority settings are used to control the supplied power. For example:

- If a device is connected to a low-priority port and causes the switch to exceed its budget, port power is not turned on.
- If a device is connected to a critical or high-priority port and causes the switch to exceed its budget, port power is turned on, but the switch drops power to one or more lower-priority ports.

Command Attributes	
• **Port:**	The port number on the switch.
• **Admin Status:**	Enables PoE power on the port. Power is automatically supplied when a device is detected on the port, providing that the power demanded does not exceed the switch or port power budget. • Default: Enabled
• **Priority:**	Sets the power priority for the port. • Options: Low, High, or Critical • Default: Low
• **Power Allocation:**	Sets the power budget for the port. • Range: 3000- 15400 milliwatts • Default: 15400 milliwatts

Configuring Port PoE Power - Web

Click PoE, Power Port Configuration. Enable PoE power on selected ports, set the priority and the power budget, and then click **Apply**.



Power Port Configuration

Port	Admin Status	Priority	Power Allocation (3000-15400 milliwatts)
1	☑ Enabled	low	13000
2	☑ Enabled	critical	15400
3	☑ Enabled	low	15000
4	☑ Enabled	high	15200
5	☑ Enabled	high	15200

FIG. 111 Web - Port Power Configuration

Configuring Port PoE Power - CLI

This example sets the PoE power budget for port 1 to 8 watts, the priority to high (2), and then enables the power.

```
Console(config)#interface ethernet 1/1300
Console(config-if)#power inline maximum allocation 8000241
Console(config-if)#power inline priority 2241
Console(config-if)#power inline auto240
Console(config-if)#
```

Address Table Settings

Overview

Switches store the addresses for all known devices. This information is used to route 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.

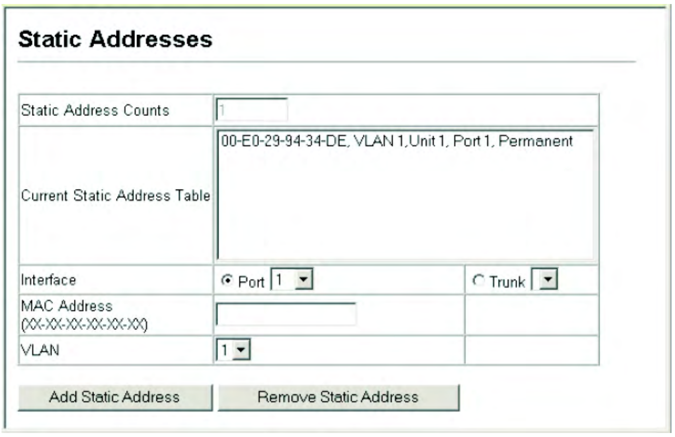
Setting Static Addresses

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.

Command Attributes	
• **Static Address Counts:**	The number of manually configured addresses. Web Only
• **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.
• **VLAN:**	ID of configured VLAN (1-4094).

Setting Static Addresses - Web

Click Address Table, Static Addresses. Specify the interface, the MAC address and VLAN, then click **Add Static Address**.



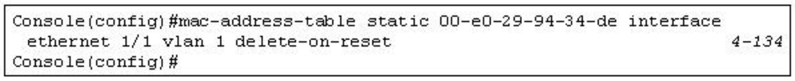
Static Addresses

Static Address Counts	1	
Current Static Address Table	00-E0-29-94-34-DE, VLAN 1,Unit 1, Port 1, Permanent	
Interface	● Port 1	○ Trunk
MAC Address (XX-XX-XX-XX-XX-XX)		
VLAN	1	

FIG. 112 Web -Configuring a Static Address Table

Setting Static Addresses - CLI

This example adds an address to the static address table, but sets it to be deleted when the switch is reset.



```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface
  ethernet 1/1 vlan 1 delete-on-reset                                4-134
Console(config)#
```

FIG. 113 CLI - Configuring a Static Address Table

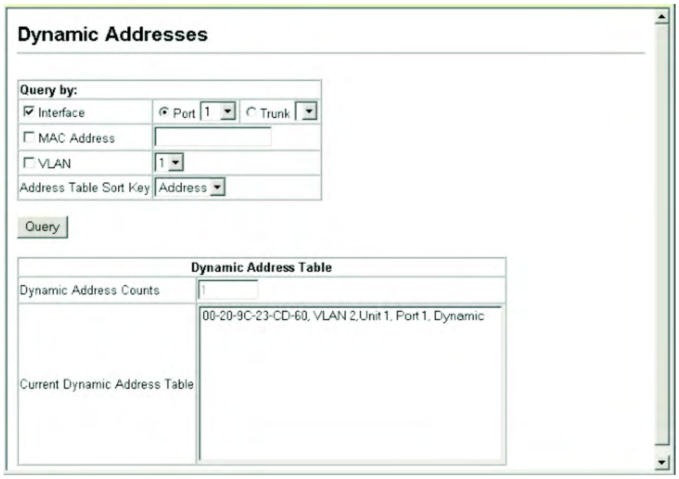
Displaying the Address Table

The Dynamic Address Table contains 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.

Command Attributes	
• **Interface:**	Indicates a port or trunk.
• **MAC Address:**	Physical address associated with this interface.
• **VLAN:**	ID of configured VLAN (1-4094).
• **Address Table Sort Key:**	You can sort the information displayed based on interface (port or trunk) or MAC address.
• **Dynamic Address Counts:**	The number of addresses dynamically learned.
• **Current Dynamic Address Table:**	Lists all the dynamic addresses.

Displaying the Address Table - Web

Click Address Table, Dynamic Addresses. Specify the search type (i.e., Interface, MAC Address, or VLAN), the method of sorting the displayed addresses, then click **Query**.



Dynamic Addresses

Query by:	
☑ Interface	● Port 1 ○ Trunk
□ MAC Address	
□ VLAN	1
Address Table Sort Key	Address

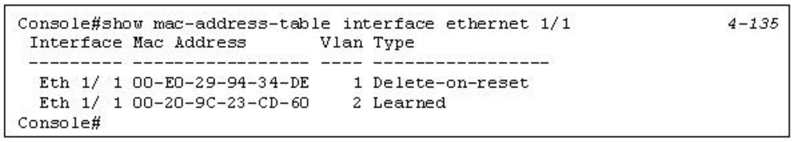
Query

Dynamic Address Table	
Dynamic Address Counts	1
Current Dynamic Address Table	00-20-9C-23-CD-60, VLAN 2,Unit 1, Port 1, Dynamic

FIG. 114 Web - Configuring a Dynamic Address Table

Displaying the Address Table - CLI

This example also displays the address table entries for port 11.



```
Console#show mac-address-table interface ethernet 1/1                4-135
 Interface Mac Address       Vlan Type
 --------- ----------------- ---- -----------------
  Eth 1/ 1 00-E0-29-94-34-DE    1 Delete-on-reset
  Eth 1/ 1 00-20-9C-23-CD-60    2 Learned
Console#
```

FIG. 115 CLI - Configuring a Dynamic Address Table

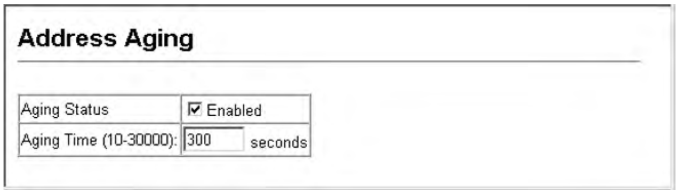
Changing the Aging Time

You can change the aging time for entries in the dynamic address table.

Command Attributes	
• **Aging Status:**	Enables or disables the aging time.
• **Aging Time:**	The time after which a learned entry is discarded. • Range: 10-1000000 seconds • Default: 300 seconds)

Changing the Aging Time - Web

Click Address Table, Address Aging. Specify the new aging time, click **Apply**.



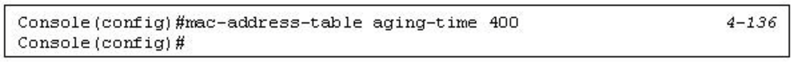
Address Aging

Aging Status	☑ Enabled
Aging Time (10-30000):	300 seconds

FIG. 116 Web - Setting the Address Aging Time

Changing the Aging Time - CLI

This example sets the aging time to 300 seconds.



```
Console(config)#mac-address-table aging-time 400                      4-136
Console(config)#
```

FIG. 117 CLI - Setting the Address Aging Time

Spanning Tree Algorithm Configuration

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)

STA uses a distributed algorithm to select a bridging device (STA-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.

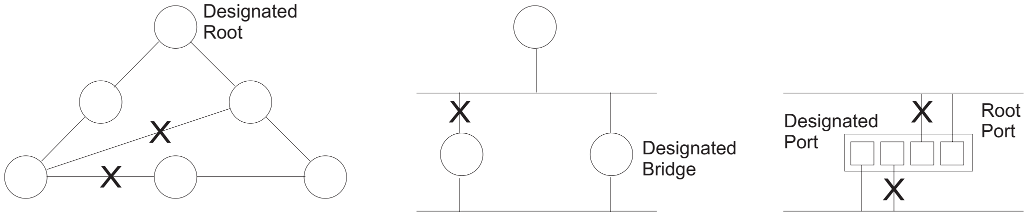


FIG. 118 Spanning Tree Algorithm Configuration

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 is designed as a general replacement for the slower, legacy STP. RSTP achieves must faster reconfiguration (i.e., around one tenth of the time required by 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.

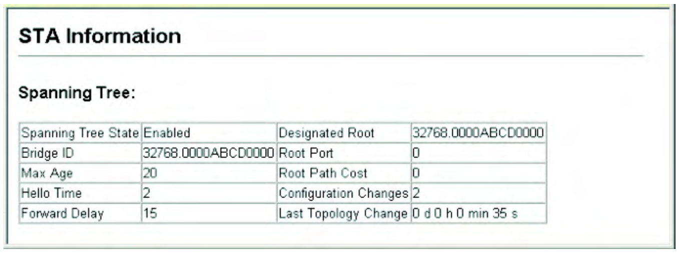
Displaying Global Settings

Field Attributes	
• **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 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. ***Note**: 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.
These additional parameters are only displayed for the CLI:	
• **Spanning tree mode:**	Specifies the type of spanning tree used on this switch: • STP: Spanning Tree Protocol (IEEE 802.1D) • RSTP: Rapid Spanning Tree (IEEE 802.1w)
• **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.
• **Root Hello Time:**	Interval (in seconds) at which this device transmits a configuration message.
• **Root Maximum Age:**	The maximum time (in seconds) this 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. If the root port ages out STA information (provided in the last configuration message), a new root port is selected from among the device ports attached to the network. ***Note**: References to "ports" in this section means "interfaces," which includes both ports and trunks.*

Field Attributes (Cont.)	
• **Root 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.
• **Transmission limit:**	The minimum interval between the transmission of consecutive RSTP BPDUs.
• **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.

Displaying Global Settings - Web

Click Spanning Tree, STA Information.



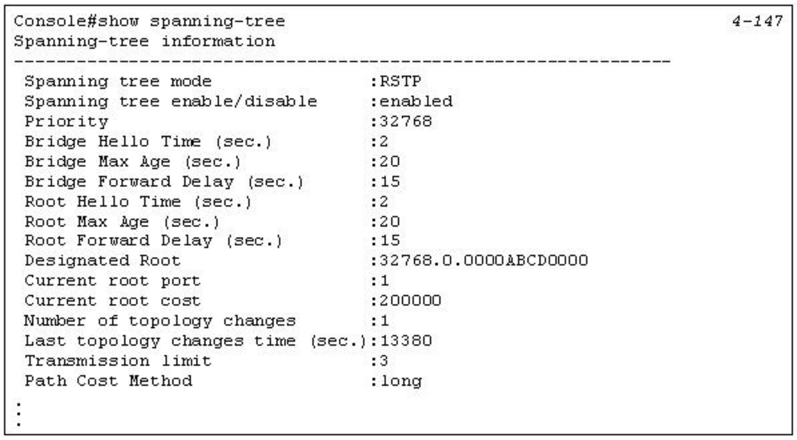
STA Information

Spanning Tree:

Spanning Tree State	Enabled	Designated Root	32768.0000ABCD0000
Bridge ID	32768.0000ABCD0000	Root Port	0
Max Age	20	Root Path Cost	0
Hello Time	2	Configuration Changes	2
Forward Delay	15	Last Topology Change	0 d 0 h 0 min 35 s

FIG. 119 Web - Displaying Spanning Tree Information

This command displays global STA settings, followed by settings for each port.



```
Console#show spanning-tree                                          4-147
Spanning-tree information
---------------------------------------------------------------
 Spanning tree mode                   :RSTP
 Spanning tree enable/disable         :enabled
 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
 Designated Root                      :32768.0.0000ABCD0000
 Current root port                    :1
 Current root cost                    :200000
 Number of topology changes           :1
 Last topology changes time (sec.):13380
 Transmission limit                   :3
 Path Cost Method                     :long
:
```

FIG. 120 CLI - Displaying Spanning Tree Information

NOTE

The current root port and current root cost display as zero when this device is not connected to the network.

Configuring Global Settings

Global settings apply to the entire switch.

Command Usage

- Spanning Tree Protocol
- Uses RSTP for the internal state machine, but sends only 802.1D BPDUs.
- 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:

NOTE

STP and RSTP BPDUs are transmitted as untagged frames, and will cross any VLAN boundaries.

- 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.

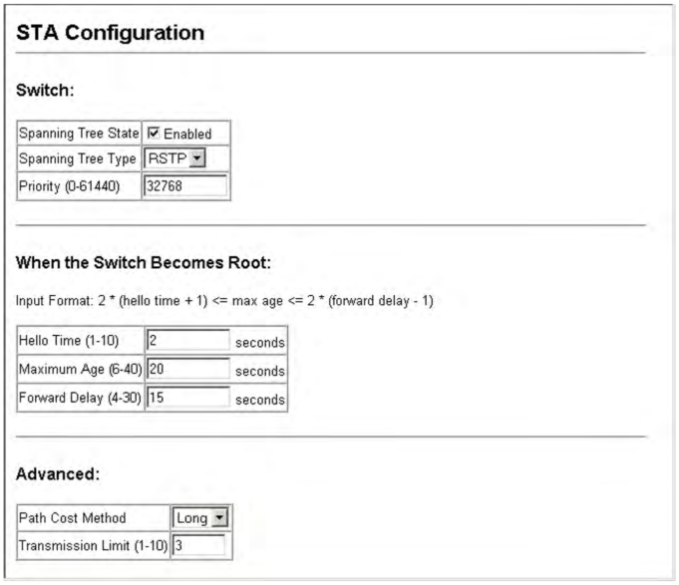
Command Attributes - Basic Configuration of Global Settings	
• **Spanning Tree State**	Enables/disables STA on this switch. (Default: Enabled)
• **Spanning Tree Type**	Specifies the type of spanning tree used on this switch: • STP: Spanning Tree Protocol (IEEE 802.1D; i.e., when this option is selected, the switch will use RSTP set to STP forced compatibility mode) • RSTP: Rapid Spanning Tree (IEEE 802.1w) RSTP is the default.
• **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. • 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

Command Attributes - Root Device Configuration	
• **Hello Time:**	Interval (in seconds) at which this 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. ***Note**: 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

Configuration Settings for RSTP	
***Note**: The following attributes apply to both STP and 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. • 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

Configuring Global Settings - Web

Click Spanning Tree, STA Configuration. Modify the required attributes, and click **Apply**.



STA Configuration

Switch:

Spanning Tree State	☑ Enabled
Spanning Tree Type	RSTP
Priority (0-61440)	32768

When the Switch Becomes Root:

Input Format: 2 * (hello time + 1) <= max age <= 2 * (forward delay - 1)

Hello Time (1-10)	2	seconds
Maximum Age (6-40)	20	seconds
Forward Delay (4-30)	15	seconds

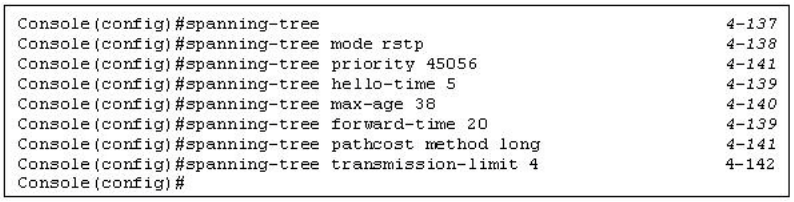
Advanced:

Path Cost Method	Long
Transmission Limit (1-10)	3

FIG. 121 Web - Configuring Spanning Tree

Configuring Global Settings - CLI

This example enables Spanning Tree Protocol, and then sets the indicated attributes.



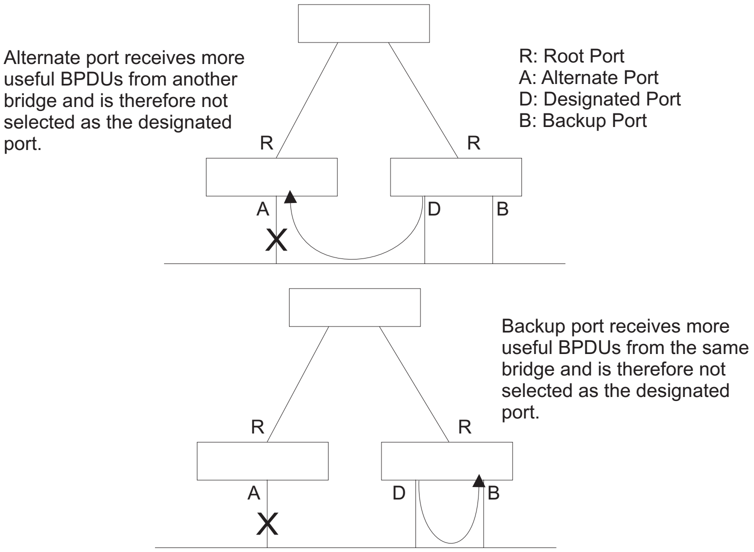
```
Console(config)#spanning-tree                                    4-137
Console(config)#spanning-tree mode rstp                          4-138
Console(config)#spanning-tree priority 45056                     4-141
Console(config)#spanning-tree hello-time 5                       4-139
Console(config)#spanning-tree max-age 38                         4-140
Console(config)#spanning-tree forward-time 20                    4-139
Console(config)#spanning-tree pathcost method long               4-141
Console(config)#spanning-tree transmission-limit 4               4-142
Console(config)#
```

FIG. 122 Web - Configuring Spanning Tree

Displaying Interface Settings

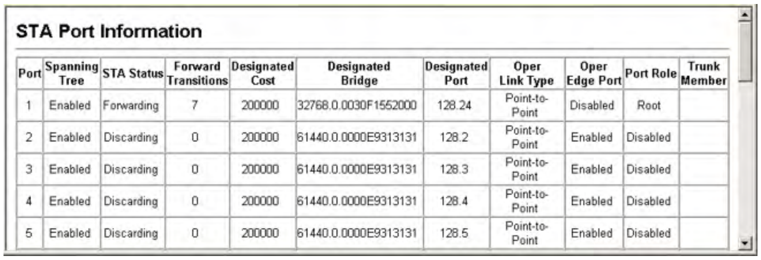
The STP Port Information and STP Trunk Information pages display the current status of ports and trunks in the Spanning Tree.

Command Attributes	
***Note**: The following attributes are read-only and cannot be changed:*	
• Spanning Tree:	Shows if STA has been enabled on this interface.
• 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 changed 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 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 120.
• Oper Edge Port:	This parameter is initialized to the setting for Admin Edge Port in STA Port Configuration on page 120 (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), or is an alternate or backup port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed.

Command Attributes (Cont.)	
• Port Role (Cont.)	The role is set to disabled (i.e., disabled port) if a port has no role within the spanning tree.  Alternate port receives more useful BPDUs from another bridge and is therefore not selected as the designated port. R: Root Port A: Alternate Port D: Designated Port B: Backup Port Backup port receives more useful BPDUs from the same bridge and is therefore not selected as the designated port.
• Trunk Member:	Indicates if a port is a member of a trunk. (STA Port Information only)
These additional parameters are only displayed for the CLI:	
• Admin Status:	Shows if this interface is enabled.
• 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. (Path cost takes precedence over port priority.)
• Priority:	Defines the priority used for this port in the Spanning Tree Algorithm. If the path cost for all ports on a switch is 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 Algorithm is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.
• Designated root:	The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
• Fast forwarding:	This field provides the same as Admin Edge port, and is only included for backward compatibility with earlier products.
• Admin Edge Port:	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 timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.
• 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.

Displaying Interface Settings - Web

Click Spanning Tree, STA Port Information or STA Trunk Information.



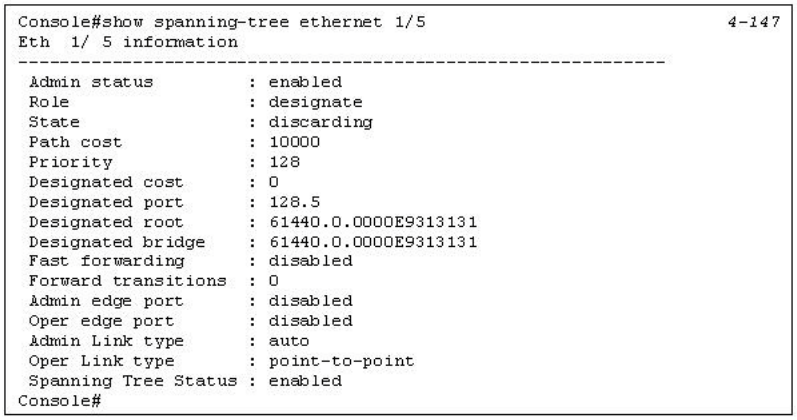
STA Port Information

Port	Spanning Tree	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Enabled	Forwarding	7	200000	32768.0.0030F1552000	128.24	Point-to-Point	Disabled	Root	
2	Enabled	Discarding	0	200000	61440.0.0000E9313131	128.2	Point-to-Point	Enabled	Disabled	
3	Enabled	Discarding	0	200000	61440.0.0000E9313131	128.3	Point-to-Point	Enabled	Disabled	
4	Enabled	Discarding	0	200000	61440.0.0000E9313131	128.4	Point-to-Point	Enabled	Disabled	
5	Enabled	Discarding	0	200000	61440.0.0000E9313131	128.5	Point-to-Point	Enabled	Disabled	

FIG. 123 Web - Displaying Spanning Tree Information

Displaying Interface Settings - CLI

This example shows general STA configuration and attributes for port 5.



```
Console#show spanning-tree ethernet 1/5                                4-147
Eth  1/ 5 information
--------------------------------------------------------------
 Admin status          : enabled
 Role                  : designate
 State                 : discarding
 Path cost             : 10000
 Priority              : 128
 Designated cost       : 0
 Designated port       : 128.5
 Designated root       : 61440.0.0000E9313131
 Designated bridge     : 61440.0.0000E9313131
 Fast forwarding       : disabled
 Forward transitions   : 0
 Admin edge port       : disabled
 Oper edge port        : disabled
 Admin Link type       : auto
 Oper Link type        : point-to-point
 Spanning Tree Status  : enabled
Console#
```

FIG. 124 CLI - Displaying Spanning Tree Information

Configuring Interface Settings

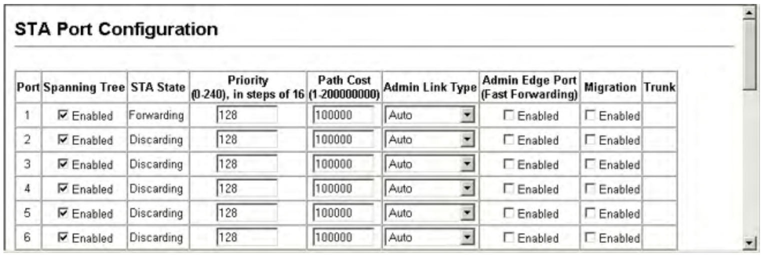
You can configure RSTP attributes for specific interfaces, including port priority, path cost, link type, and edge port. You may use a different priority or path cost for ports of the same media type to indicate the preferred path, link type to indicate a point-to-point connection or shared-media connection, 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.)

Command Attributes	
***Note**: The following attributes are read-only and cannot be changed:*	
• **Port:**	Ports only; i.e., no trunks or trunk port members.
• **STA State:**	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.
• **Trunk:**	Indicates if a port is a member of a trunk. (STA Port Configuration only)
The following interface attributes can be configured:	
• **Spanning Tree:**	Enables/disables spanning tree on a port.

Command Attributes (Cont.)	
• **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
• **Path Cost:**	This parameter is used by the STP 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 330), the maximum path cost is 65,535. • Range: • Ethernet: 200,000-20,000,000 • Fast Ethernet: 20,000-2,000,000 • Gigabit Ethernet: 2,000-200,000 • Default: • 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
• **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.)
• **Admin Edge Port** (Fast Forwarding):	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 timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device. (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

Configuring Interface Settings - Web

Click Spanning Tree, STA Port Configuration or STA Trunk Configuration. Modify the required attributes, then click **Apply**.



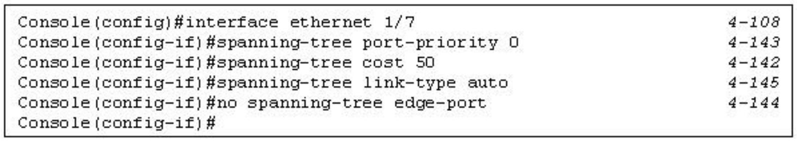
STA Port Configuration

Port	Spanning Tree	STA State	Priority (0-240), in steps of 16	Path Cost (1-200000000)	Admin Link Type	Admin Edge Port (Fast Forwarding)	Migration	Trunk
1	☑ Enabled	Forwarding	128	100000	Auto	□ Enabled	□ Enabled	
2	☑ Enabled	Discarding	128	100000	Auto	□ Enabled	□ Enabled	
3	☑ Enabled	Discarding	128	100000	Auto	□ Enabled	□ Enabled	
4	☑ Enabled	Discarding	128	100000	Auto	□ Enabled	□ Enabled	
5	☑ Enabled	Discarding	128	100000	Auto	□ Enabled	□ Enabled	
6	☑ Enabled	Discarding	128	100000	Auto	□ Enabled	□ Enabled	

FIG. 125 Web - Configuring Spanning Tree per Port

Configuring Interface Settings - CLI

This example sets STA attributes for port 5.



```
Console(config)#interface ethernet 1/7                                4-108
Console(config-if)#spanning-tree port-priority 0                      4-143
Console(config-if)#spanning-tree cost 50                              4-142
Console(config-if)#spanning-tree link-type auto                       4-145
Console(config-if)#no spanning-tree edge-port                         4-144
Console(config-if)#
```

FIG. 126 Web - Configuring Spanning Tree per Port

VLAN Configuration

Overview - 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 MAX).

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

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.

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 (FIG. 127).

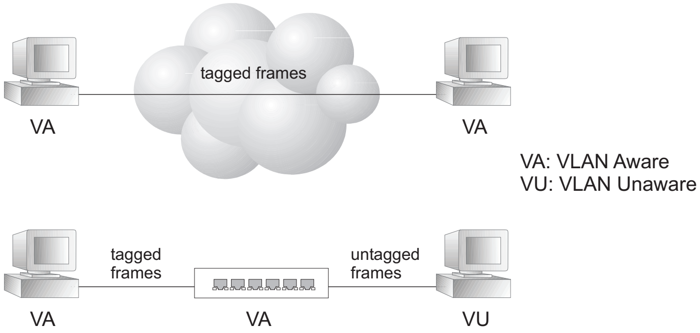


FIG. 127 Assigning Ports to VLANs

- **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 (or static) 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 endstation 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 ports to prevent advertisements being propagated, or forbid ports from joining restricted VLANs.

  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 the *Adding Static Members to VLANs (VLAN Index)* section on page 128). But you can still enable GVRP on these edge switches, as well as on the core switches in the network (FIG. 128).

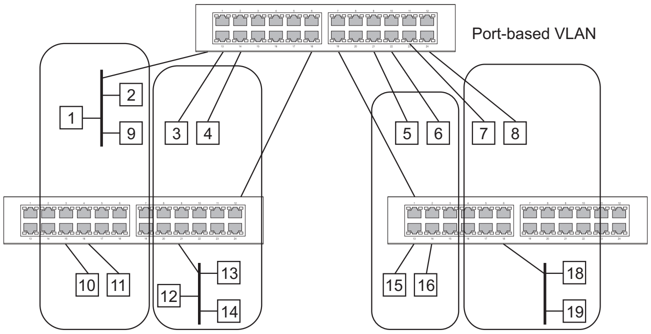


FIG. 128 Security Boundaries

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.

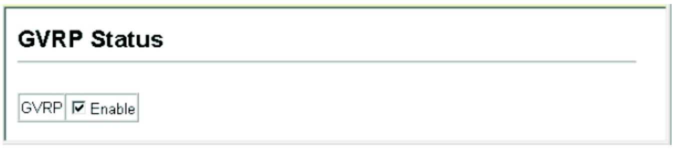
Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is therefore capable of passing tagged or untagged frames. When forwarding a frame from this switch along a path that contains any VLAN-aware devices, the switch should include VLAN tags. When forwarding a frame from 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.

Enabling or Disabling GVRP (Global Setting)

GARP VLAN Registration Protocol (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).

Enabling or Disabling GVRP - Web

Click VLAN, 802.1Q VLAN, GVRP Status. Enable or disable GVRP, and click **Apply**.



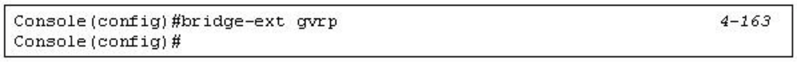
GVRP Status

GVRP ☑ Enable

FIG. 129 Web - Enabling GVRP

Enabling or Disabling GVRP - CLI

This example enables GVRP for the switch.



```
Console(config)#bridge-ext gvrp                                    4-163
Console(config)#
```

FIG. 130 CLI - Enabling GVRP

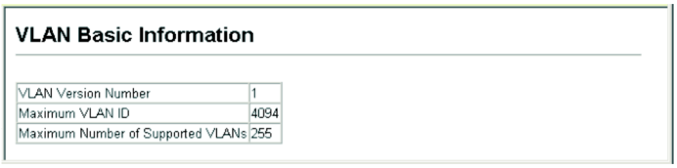
Displaying Basic VLAN Information

The VLAN Basic Information page displays basic information on the VLAN type supported by the switch.

Field Attributes	
• **VLAN Version Number:**	The VLAN version used by this switch as specified in the IEEE 802.1Q standard. Web only.
• **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.

Displaying Basic VLAN Information - Web

Click VLAN, 802.1Q VLAN, VLAN Base Information.



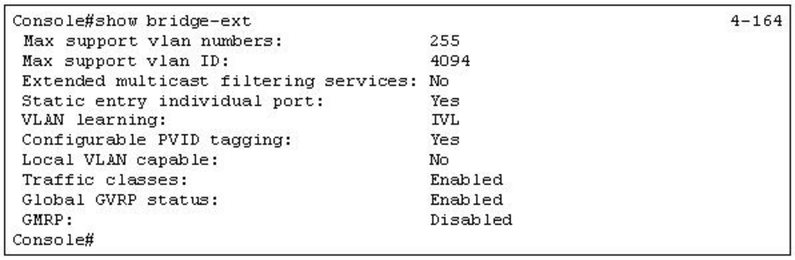
VLAN Basic Information

VLAN Version Number	1
Maximum VLAN ID	4094
Maximum Number of Supported VLANs	255

FIG. 131 Web - Displaying Basic VLAN information

Displaying Basic VLAN Information - CLI

Enter the following command.



```
Console#show bridge-ext                                          4-164
 Max support vlan numbers:              255
 Max support 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:                    Enabled
 GMRP:                                  Disabled
Console#
```

FIG. 132 CLI - Displaying Basic VLAN information

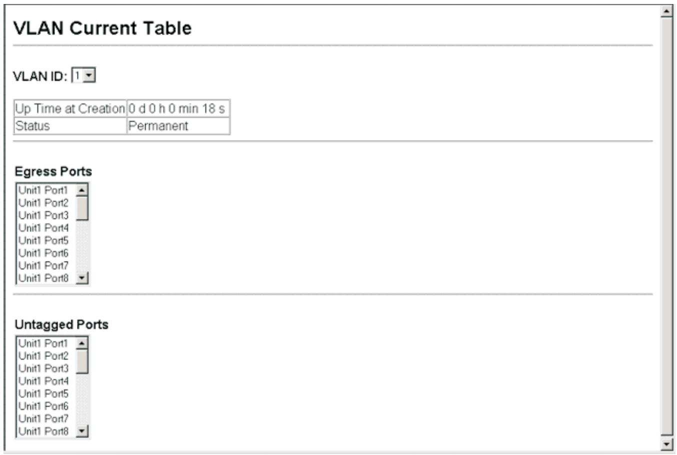
Displaying Current VLANs

The VLAN Current Table 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.

Command Attributes - Web	
• **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.

Displaying Current VLANs - Web

Click VLAN, 802.1Q VLAN, Current Table. Select any ID from the scroll-down list.



VLAN Current Table

VLAN ID: 1

Up Time at Creation	0 d 0 h 0 min 18 s
Status	Permanent

Egress Ports

Unit1 Port1
Unit1 Port2
Unit1 Port3
Unit1 Port4
Unit1 Port5
Unit1 Port6
Unit1 Port7
Unit1 Port8

Untagged Ports

Unit1 Port1
Unit1 Port2
Unit1 Port3
Unit1 Port4
Unit1 Port5
Unit1 Port6
Unit1 Port7
Unit1 Port8

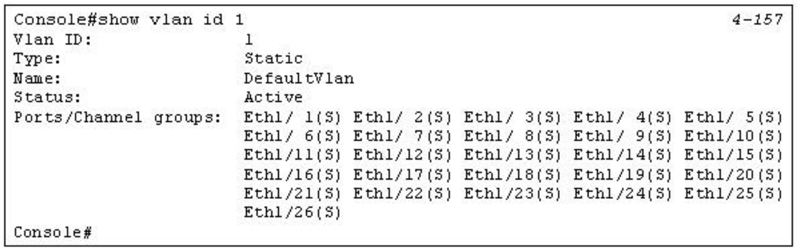
FIG. 133 Web - Displaying Current VLANs

Command Attributes - CLI	
• **VLAN:**	ID of configured VLAN (1-4094, no leading zeroes).
• **Type:**	Shows how this VLAN was added to the switch. • Dynamic: Automatically learned via GVRP. • Static: Added as a static entry.
• **Name:**	Name of the VLAN (1 to 32 characters).

• **Status:**	Shows if this VLAN is enabled or disabled. • Active: VLAN is operational. • Suspend: VLAN is suspended; i.e., does not pass packets.
• **Ports / Channel Groups:**	Shows the VLAN interface members.

Displaying Current VLANs - CLI

Current VLAN information can be displayed with the following command.



```
Console#show vlan id 1                                              4-157
Vlan ID:                   1
Type:                      Static
Name:                      DefaultVlan
Status:                    Active
Ports/Channel groups:      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)
Console#
```

FIG. 134 CLI - Displaying Current VLANs

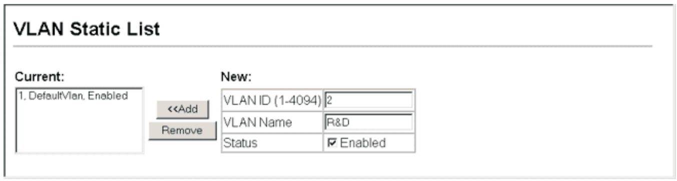
Creating VLANs

Use the VLAN Static List 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.

Command Attributes	
• **Current:**	Lists all the current VLAN groups created for this system. Up to 255 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.
• **New:**	Allows you to specify the name and numeric identifier for a new VLAN group. (The VLAN name is only used for management on this system; it is not added to the VLAN tag.)
• **VLAN ID:**	ID of configured VLAN (1-4094, no leading zeroes).
• **VLAN Name:**	Name of the VLAN (1 to 32 characters).
• **Status (Web):**	Enables or disables the specified VLAN. • Enable: VLAN is operational. • Disable: VLAN is suspended; i.e., does not pass packets.
• **State (CLI):**	Enables or disables the specified VLAN. • Active: VLAN is operational. • Suspend: VLAN is suspended; i.e., does not pass packets.
• **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.

Creating VLANs - Web

Click VLAN, 802.1Q VLAN, Static List. To create a new VLAN, enter the VLAN ID and VLAN name, mark the Enable checkbox to activate the VLAN, and then click **Add**.



VLAN Static List

Current:

1, DefaultVlan, Enabled

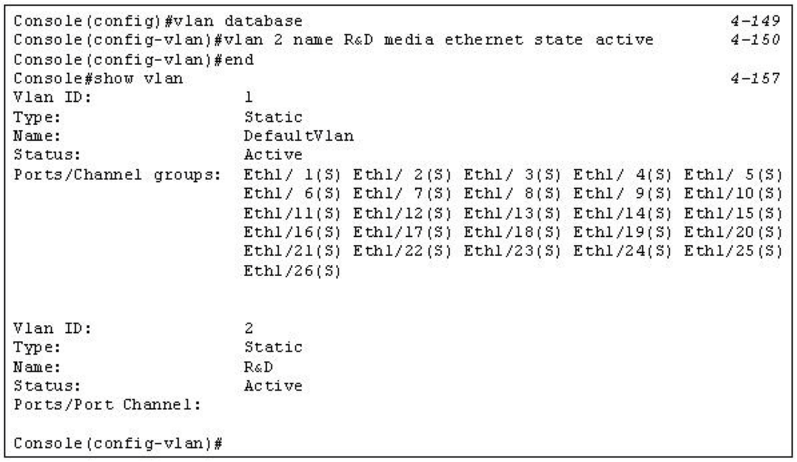
New:

VLAN ID (1-4094)	2
VLAN Name	R&D
Status	☑ Enabled

FIG. 135 Web - Configuring a VLAN Static List

Creating VLANs - CLI

This example creates a new VLAN.



```
Console(config)#vlan database                                         4-149
Console(config-vlan)#vlan 2 name R&D media ethernet state active      4-150
Console(config-vlan)#end
Console#show vlan                                                     4-157
Vlan ID:                 1
Type:                    Static
Name:                    DefaultVlan
Status:                  Active
Ports/Channel groups:    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)


Vlan ID:                 2
Type:                    Static
Name:                    R&D
Status:                  Active
Ports/Port Channel:

Console(config-vlan)#
```

FIG. 136 CLI - Configuring a VLAN Static List

Adding Static Members to VLANs (VLAN Index)

Use the VLAN Static Table to configure port members for the selected VLAN index.

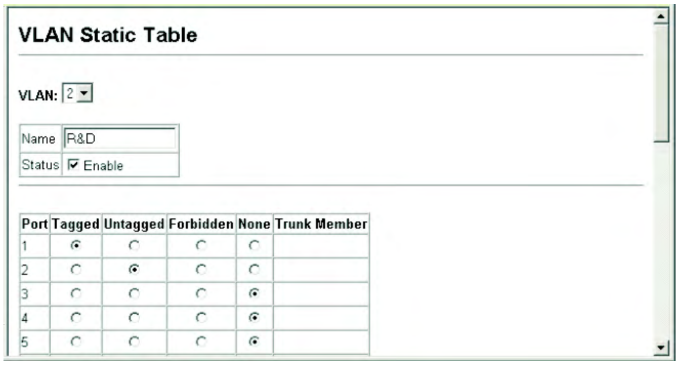
Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices, or untagged they are not connected to any VLAN-aware devices. Or configure a port as forbidden to prevent the switch from automatically adding it to a VLAN via the GVRP protocol.

1. You can also use the VLAN Static Membership by Port page to configure VLAN groups based on the port index (page 129). However, note that this configuration page can only add ports to a VLAN as tagged members.
2. VLAN 1 is the default untagged VLAN containing all ports on the switch, and can only be modified by first reassigning the default port VLAN ID as described under *Configuring VLAN Behavior for Interfaces* section on page 130.

Command Attributes	
• **VLAN:**	ID of configured VLAN (1-4094, no leading zeroes).
• **Name:**	Name of the VLAN (1 to 32 characters).
• **Status:**	Enables or disables the specified VLAN. • Enable: VLAN is operational. • Disable: VLAN is suspended; i.e., does not pass packets.
• **Port:**	Port identifier.
• **Trunk:**	Trunk identifier.
• **Membership Type:**	Select VLAN membership for each interface by marking the appropriate radio button for a port or trunk: • 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 124. • None: Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.
• **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.

Adding Static Members to VLANs - Web

Click VLAN, 802.1Q VLAN, Static Table. 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. Click **Apply**.



VLAN Static Table

VLAN: 2

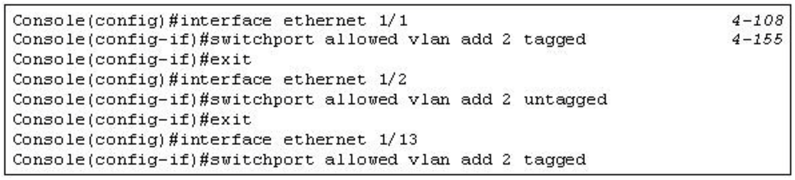
Name	R&D
Status	☑ Enable

Port	Tagged	Untagged	Forbidden	None	Trunk Member
1	●	○	○	○	
2	○	●	○	○	
3	○	○	○	●	
4	○	○	○	●	
5	○	○	○	●	

FIG. 137 Web - Configuring a VLAN Static Table

Adding Static Members to VLANs - CLI

The following example adds tagged and untagged ports to VLAN 2.



```
Console(config)#interface ethernet 1/1                              4-108
Console(config-if)#switchport allowed vlan add 2 tagged             4-155
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#switchport allowed vlan add 2 untagged
Console(config-if)#exit
Console(config)#interface ethernet 1/13
Console(config-if)#switchport allowed vlan add 2 tagged
```

FIG. 138 CLI - Configuring a VLAN Static Table

Adding Static Members to VLANs (Port Index)

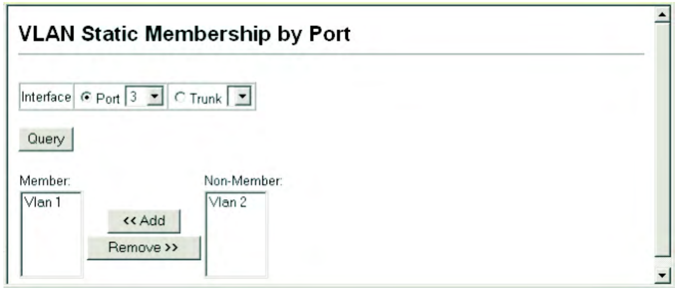
Use the VLAN Static Membership by Port menu to assign VLAN groups to the selected interface as a tagged member.

Command Attributes	
• **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.

Adding Static Members to VLANs - Web

Click VLAN, 802.1Q VLAN, VLAN Static Membership. Select an interface from the scroll-down box (Port or Trunk). Click Query to display membership information for the interface. Select a VLAN ID, and then click Add to add the interface as a tagged member, or click Remove to remove the interface.

After configuring VLAN membership for each interface, click **Apply**.



VLAN Static Membership by Port

Interface ● Port 3 ○ Trunk

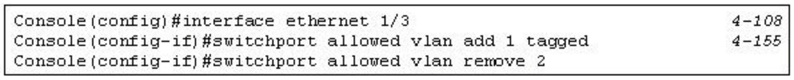
Member: Vlan 1

Non-Member: Vlan 2

FIG. 139 Web - VLAN Static Membership by Port

Adding Static Members to VLANs - CLI

This example adds Port 3 to VLAN 1 as a tagged port, and removes Port 3 from VLAN 2.



```
Console(config)#interface ethernet 1/3                                4-108
Console(config-if)#switchport allowed vlan add 1 tagged               4-155
Console(config-if)#switchport allowed vlan remove 2
```

FIG. 140 CLI - VLAN Static Membership by Port

Configuring VLAN Behavior for Interfaces

You can configure VLAN behavior for specific interfaces, including the default VLAN identifier (PVID), accepted frame types, ingress filtering, GVRP status, and GARP timers.

Command Usage

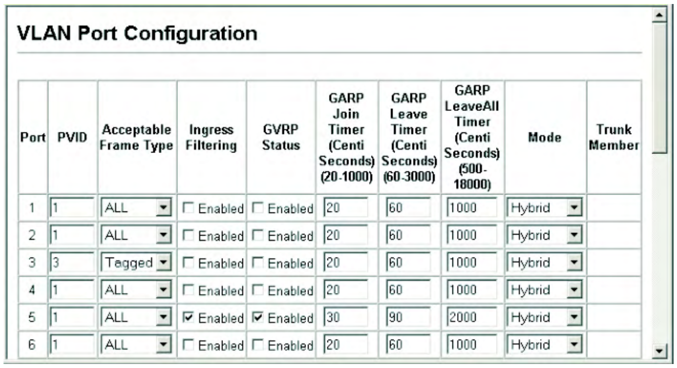
- **GVRP** – GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network.
- **GARP** – Group Address Registration Protocol is used by GVRP and GMRP to register or deregister client attributes 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.

Command Attributes	
• **PVI:**	VLAN ID assigned to untagged frames received on the interface. • Default: 1 • If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.
• **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. • Option: All, Tagged • Default: All
• **Ingress Filtering:**	If ingress filtering is enabled, incoming frames for VLANs which do not include this ingress port in their member set will be discarded at the ingress port. However, they do affect VLAN dependent BPDU frames, such as GMRP.(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.
• **GVRP Status:**	Enables/disables GVRP for the interface. GVRP must be globally enabled for the switch before this setting can take effect. (See the *Displaying Bridge Extension Capabilities* section on page 27.) 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 Join Timer:**	The interval between transmitting requests/queries to participate in a VLAN group. • Range: 20-1000 centiseconds • Default: 20 • Timer settings must follow this rule: 2 x (join timer) < leave timer < leaveAll timer

Command Attributes (Cont.)	
• **GARP Leave Timer:**	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 • Timer settings must follow this rule: 2 x (join timer) < leave timer < leaveAll timer
• **GARP LeaveAll Timer:**	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 • Timer settings must follow this rule: 2 x (join timer) < leave timer < leaveAll timer
• **Mode:**	Indicates VLAN membership mode for an interface. (Default: 1Q Trunk) • 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. • Hybrid – Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.
• **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.

Configuring VLAN Behavior for Interfaces - Web

Click VLAN, 802.1Q VLAN, Port Configuration or Trunk Configuration. Fill in the required settings for each interface, click **Apply**.



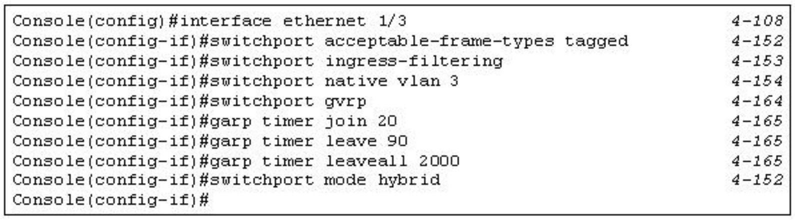
VLAN Port Configuration

Port	PVID	Acceptable Frame Type	Ingress Filtering	GVRP Status	GARP Join Timer (Centi Seconds) (20-1000)	GARP Leave Timer (Centi Seconds) (60-3000)	GARP LeaveAll Timer (Centi Seconds) (500-18000)	Mode	Trunk Member
1	1	ALL	□ Enabled	□ Enabled	20	60	1000	Hybrid	
2	1	ALL	□ Enabled	□ Enabled	20	60	1000	Hybrid	
3	3	Tagged	□ Enabled	□ Enabled	20	60	1000	Hybrid	
4	1	ALL	□ Enabled	□ Enabled	20	60	1000	Hybrid	
5	1	ALL	☑ Enabled	☑ Enabled	30	90	2000	Hybrid	
6	1	ALL	□ Enabled	□ Enabled	20	60	1000	Hybrid	

FIG. 141 Web - Configuring VLANs per Port

Configuring VLAN Behavior for Interfaces - CLI

This example sets port 1 to accept only tagged frames, assigns PVID 3 as the native VLAN ID, enables GVRP, sets the GARP timers, and then sets the switchport mode to hybrid.



```
Console(config)#interface ethernet 1/3                              4-108
Console(config-if)#switchport acceptable-frame-types tagged         4-152
Console(config-if)#switchport ingress-filtering                     4-153
Console(config-if)#switchport native vlan 3                         4-154
Console(config-if)#switchport gvrp                                  4-164
Console(config-if)#garp timer join 20                               4-165
Console(config-if)#garp timer leave 90                              4-165
Console(config-if)#garp timer leaveall 2000                         4-165
Console(config-if)#switchport mode hybrid                           4-152
Console(config-if)#
```

FIG. 142 CLI - Configuring VLANs per Port

Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. This switch supports two types of private VLAN ports: promiscuous, and community ports. A promiscuous port can communicate with all interfaces within a private VLAN. Community ports can only communicate with other ports in their own community VLAN, and with their designated promiscuous ports. (Note that private VLANs and normal VLANs can exist simultaneously within the same switch.)

Each private VLAN consists of two components: a primary VLAN and one or more community VLANs. A primary VLAN allows traffic to pass between promiscuous ports, and between promiscuous ports and community ports subordinate to the primary VLAN. A community VLAN conveys traffic between community ports, and from the community ports to their associated promiscuous ports. Multiple primary VLANs can be configured on this switch, and multiple community VLANs can be configured within each primary VLAN.

To configure private VLANs, follow these steps:

1. Use the Private VLAN Configuration menu (page 133) 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 menu (page 133) to map the secondary (i.e., community) VLAN(s) to the primary VLAN.
3. Use the Private VLAN Port Configuration menu (page 135) 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 a promiscuous port). Then assign any promiscuous ports to a primary VLAN and any host ports a secondary VLAN (i.e., community VLAN).

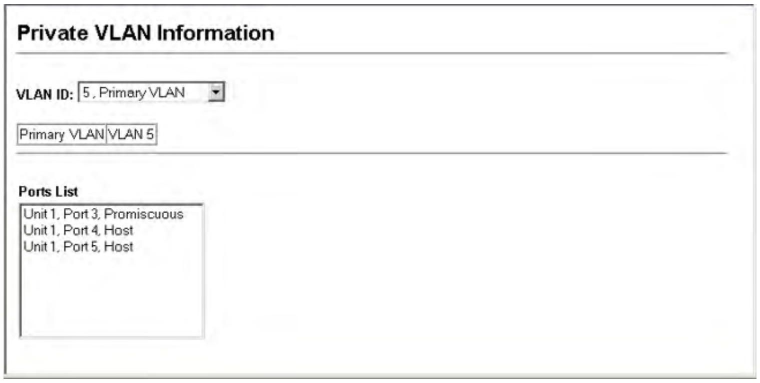
Displaying Current Private VLANs

The Private VLAN Information page displays information on the private VLANs configured on the switch, including primary and community VLANs, and their associated interfaces.

Command Attributes	
• **VLAN ID:**	ID of configured VLAN (1-4093, no leading zeroes).
• **Primary VLAN:**	The primary VLAN with which the selected VLAN is associated. (Note that this displays as VLAN 0 if the selected VLAN is itself a primary VLAN.)
• **Ports List:**	The list of ports (and assigned type) in the selected private VLAN.

Displaying Current Private VLANs - Web

Click Private VLAN, Private VLAN Information. Select the desired port from the VLAN ID drop-down menu.



Private VLAN Information

VLAN ID: 5, Primary VLAN

Primary VLAN VLAN 5

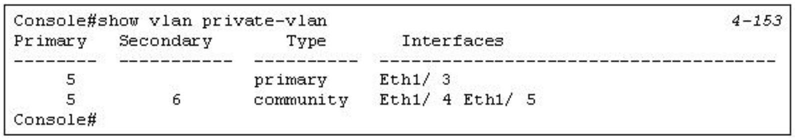
Ports List

Unit 1, Port 3, Promiscuous
Unit 1, Port 4, Host
Unit 1, Port 5, Host

FIG. 143 Web - Private VLAN Information

Displaying Current Private VLANs - CLI

This example shows the switch configured with primary VLAN 5 and secondary VLAN 6. Port 3 has been configured as a promiscuous port and mapped to VLAN 5, while ports 4 and 5 have been configured as a host ports and are associated with VLAN 6. This means that traffic for port 4 and 5 can only pass through port 3.



```
Console#show vlan private-vlan                                        4-153
Primary   Secondary       Type       Interfaces
--------  -----------  ----------  --------------------------------------
     5                 primary     Eth1/ 3
     5         6       community   Eth1/ 4 Eth1/ 5
Console#
```

FIG. 144 CLI - Private VLAN Information

Configuring Private VLANs

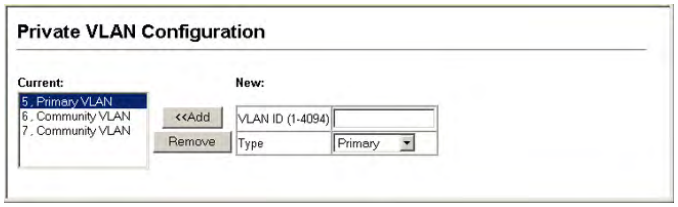
The Private VLAN Configuration page is used to create/remove primary or community VLANs.

Command Attributes	
• **VLAN ID:**	ID of configured VLAN (1-4094, no leading zeroes).
• **Type:**	There are two types of VLANs within a private VLAN: • Primary VLANs - Conveys traffic between promiscuous ports, and to community ports within secondary VLANs. • Community VLANs - Conveys traffic between community ports, and to their associated promiscuous ports.
• **Current:**	Displays a list of the currently configured VLANs.

Configuring Private VLANs - Web

Click Private VLAN, Private VLAN Configuration. Enter the VLAN ID number, select Primary or Community type, then click Add. To remove a private VLAN from the switch, highlight an entry in the Current list box and then click Remove.

Note that all member ports must be removed from the VLAN before it can be deleted.



Private VLAN Configuration

Current:

5 , Primary VLAN
6 , Community VLAN
7 , Community VLAN

New:

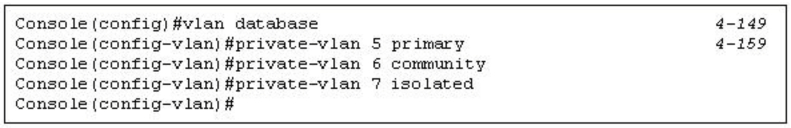
VLAN ID (1-4094)

Type: Primary

FIG. 145 Web - Private VLAN Configuration

Configuring Private VLANs - CLI

This example configures VLAN 5 as a primary VLAN, and VLAN 6 and 7 as community VLANs.



```
Console(config)#vlan database                                     4-149
Console(config-vlan)#private-vlan 5 primary                       4-159
Console(config-vlan)#private-vlan 6 community
Console(config-vlan)#private-vlan 7 isolated
Console(config-vlan)#
```

FIG. 146 CLI - Private VLAN Configuration

Associating Community VLANs

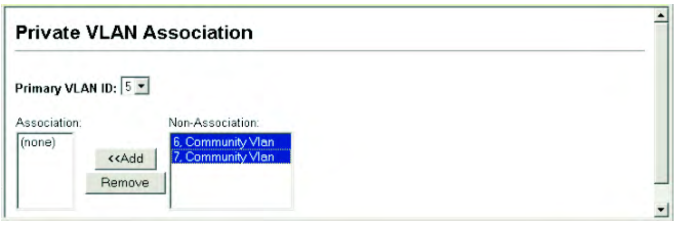
Each community VLAN must be associated with a primary VLAN.

Command Attributes	
• **Primary VLAN ID:**	ID of primary VLAN (1-4094, no leading zeroes).
• **Association:**	Community VLANs associated with the selected primary VLAN.
• **Non-Association:**	Community VLANs not associated with the selected primary VLAN.

Associating Community VLANs - Web

Click Private VLAN, Private VLAN Association. Select the required primary VLAN from the scroll-down box, highlight one or more community VLANs in the Non-Association list box, and click Add to associate these entries with the selected primary VLAN.

A community VLAN can only be associated with one primary VLAN.



Private VLAN Association

Primary VLAN ID: 5

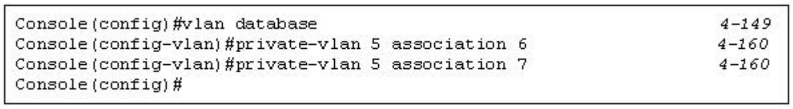
Association: (none)

Non-Association: 6, Community Vlan
7, Community Vlan

FIG. 147 Web - Private VLAN Association

Associating Community VLANs - CLI

This example associates community VLANs 6 and 7 with primary VLAN 5.



```
Console(config)#vlan database                                          4-149
Console(config-vlan)#private-vlan 5 association 6                      4-160
Console(config-vlan)#private-vlan 5 association 7                      4-160
Console(config)#
```

FIG. 148 CLI - Private VLAN Association

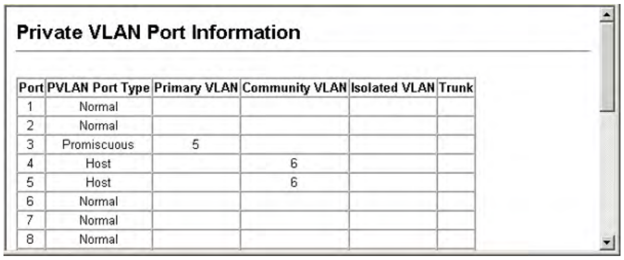
Displaying Private VLAN Interface Information

Use the Private VLAN Port Information and Private VLAN Trunk Information menus to display the interfaces associated with private VLANs.

Command Attributes	
• **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). • 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.
• **Secondary VLAN:**	On this switch all secondary VLANs are community VLANs. A community VLAN conveys traffic between community ports, and from community ports to their designated promiscuous ports.
• **Trunk:**	The trunk identifier. (Private VLAN Port Information only)

Displaying Private VLAN Interface Information - Web

Click Private VLAN, Private VLAN Port Information or Private VLAN Trunk Information.



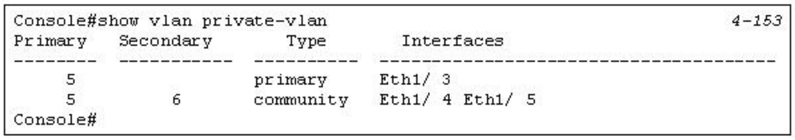
Private VLAN Port Information

Port	PVLAN Port Type	Primary VLAN	Community VLAN	Isolated VLAN	Trunk
1	Normal				
2	Normal				
3	Promiscuous	5			
4	Host		6		
5	Host		6		
6	Normal				
7	Normal				
8	Normal				

FIG. 149 Web - Displaying Private VLAN Port Information

Displaying Private VLAN Interface Information - CLI

This example shows the switch configured with primary VLAN 5 and secondary VLAN 6. Port 3 has been configured as a promiscuous port and mapped to VLAN 5, while ports 4 and 5 have been configured as a host ports and associated with VLAN 6. This means that traffic for port 4 and 5 can only pass through port 3.



```
Console#show vlan private-vlan                                              4-153
Primary   Secondary       Type       Interfaces
--------  -----------  ----------  --------------------------------------
    5                   primary     Eth1/ 3
    5          6        community   Eth1/ 4 Eth1/ 5
Console#
```

FIG. 150 CLI - Displaying Private VLAN Port Information

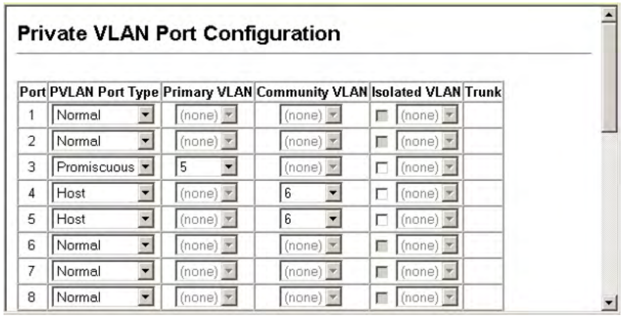
Configuring Private VLAN Interfaces

Use the Private VLAN Port Configuration and Private VLAN Trunk Configuration menus to set the private VLAN interface type, and associate the interfaces with a private VLAN.

Command Attributes	
• **Port/Trunk:**	The switch interface.
• **PVLAN Port Type:**	Sets the private VLAN port types. • Normal – The port is not configured into 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). • 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 PVLAN type is “Promiscuous,” then specify the associated primary VLAN. For “Host” type, the Primary VLAN displayed is the one to which the selected secondary VLAN has been associated.
• **Secondary VLAN:**	On this switch, all secondary VLANs are community VLANs. A community VLAN conveys traffic between community ports, and from community ports to their designated promiscuous ports. If PVLAN Port Type is “Host,” then specify the associated secondary VLAN.

Configuring Private VLAN Interfaces - Web

Click Private VLAN, Private VLAN Port Configuration or Private VLAN Trunk Configuration. Set the PVLAN Port Type for each port that will join a private VLAN. For promiscuous ports, set the associated primary VLAN. For host ports, set the associated secondary VLAN. After all the ports have been configured, click **Apply**.



Private VLAN Port Configuration

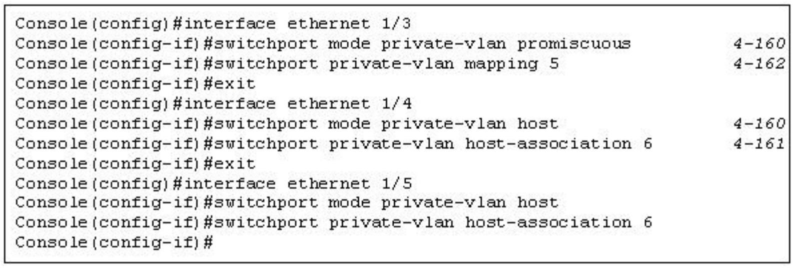
Port	PVLAN Port Type	Primary VLAN	Community VLAN	Isolated VLAN	Trunk
1	Normal	(none)	(none)	□ (none)	
2	Normal	(none)	(none)	□ (none)	
3	Promiscuous	5	(none)	□ (none)	
4	Host	(none)	6	□ (none)	
5	Host	(none)	6	□ (none)	
6	Normal	(none)	(none)	□ (none)	
7	Normal	(none)	(none)	□ (none)	
8	Normal	(none)	(none)	□ (none)	

FIG. 151 Web - Private VLAN Port Configuration

Configuring Private VLAN Interfaces - CLI

This example shows the switch configured with primary VLAN 5 and secondary VLAN 6.

Port 3 has been configured as a promiscuous port and mapped to VLAN 5, while ports 4 and 5 have been configured as a host ports and associated with VLAN 6. This means that traffic for port 4 and 5 can only pass through port 3.



```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport mode private-vlan promiscuous         4-160
Console(config-if)#switchport private-vlan mapping 5                4-162
Console(config-if)#exit
Console(config)#interface ethernet 1/4
Console(config-if)#switchport mode private-vlan host                4-160
Console(config-if)#switchport private-vlan host-association 6       4-161
Console(config-if)#exit
Console(config)#interface ethernet 1/5
Console(config-if)#switchport mode private-vlan host
Console(config-if)#switchport private-vlan host-association 6
Console(config-if)#
```

FIG. 152 CLI - Private VLAN Port Configuration

Class of Service Configuration

Overview

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 is designed with CoS to specifically support AMX's MAX audio and video streams, maximizing audio and video performance as it is transmitted throughout the network. With four priority queues for each port, MAX's packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can change the default priority for each interface, and configure the mapping of frame priority tags to the switch's priority queues.

For MAX, AMX has pre-configured the A/V traffic so the switch automatically supports MAX without any additional configuration.

Setting the Default Priority for Interfaces

You can 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.

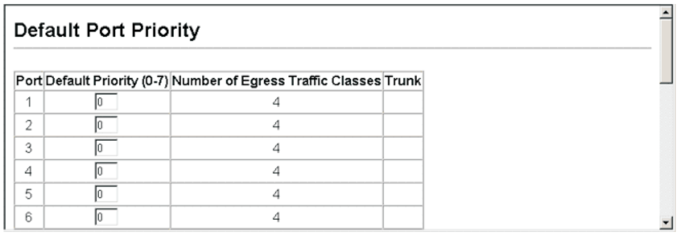
Command Usage

- 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.

Command Attributes	
• **Default Priority:**	The priority that is assigned to untagged frames received on the specified interface. • Range: 0 - 7 • Default: 0 CLI displays this information as "Priority for untagged traffic."
• **Number of Egress Traffic Classes:**	• The number of queue buffers provided for each port.

Setting the Default Priority for Interfaces - Web

Click Priority, Default Port Priority or Default Trunk Priority. Modify the default priority for any interface, then click **Apply**.



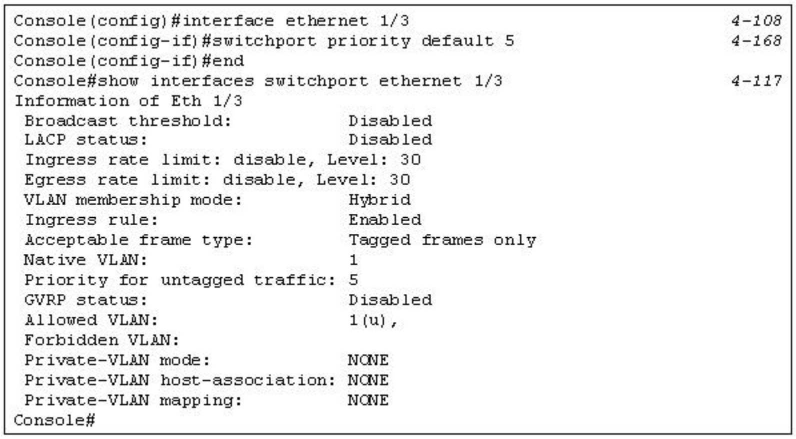
Default Port Priority

Port	Default Priority (0-7)	Number of Egress Traffic Classes	Trunk
1	0	4	
2	0	4	
3	0	4	
4	0	4	
5	0	4	
6	0	4	

FIG. 153 Web - Port Priority Configuration

Setting the Default Priority for Interfaces - CLI

This example assigns a default priority of 5 to port 3.



```
Console(config)#interface ethernet 1/3                                    4-108
Console(config-if)#switchport priority default 5                          4-168
Console(config-if)#end
Console#show interfaces switchport ethernet 1/3                           4-117
Information of Eth 1/3
 Broadcast threshold:            Disabled
 LACP status:                    Disabled
 Ingress rate limit: disable, Level: 30
 Egress rate limit: disable, Level: 30
 VLAN membership mode:           Hybrid
 Ingress rule:                   Enabled
 Acceptable frame type:          Tagged frames only
 Native VLAN:                    1
 Priority for untagged traffic:  5
 GVRP status:                    Disabled
 Allowed VLAN:                   1(u),
 Forbidden VLAN:
 Private-VLAN mode:              NONE
 Private-VLAN host-association:  NONE
 Private-VLAN mapping:           NONE
Console#
```

FIG. 154 CLI - Port Priority Configuration

Mapping CoS Values to Egress Queues

This switch processes Class of Service (CoS) priority tagged traffic by using four priority queues for each port, with service schedules based on Weighted Round Robin (WRR). Up to 8 separate traffic priorities are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

Egress Queue Priority Mapping				
Queue	0	1	2	3
Priority	1,2	0,3	4,5	6,7

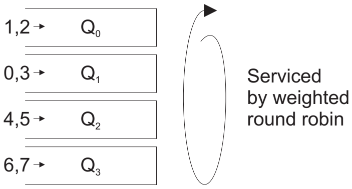


FIG. 155 Weighted Round Robin (WRR)

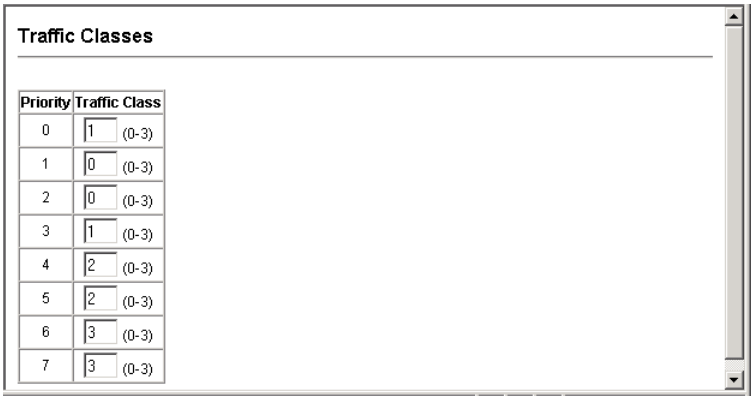
The priority levels recommended in the IEEE 802.1p standard for various network applications are shown in the following table. However, you can map the priority levels to the switch's output queues in any way that benefits application traffic for your own network.

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

Command Attributes	
• **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 • CLI shows Queue ID.

Mapping CoS Values to Egress Queues - Web

Click Priority, Traffic Classes. Mark an interface and click Select to display the current mapping of CoS values to output queues. Assign priorities to the traffic classes (i.e., output queues) for the selected interface, then click **Apply**.



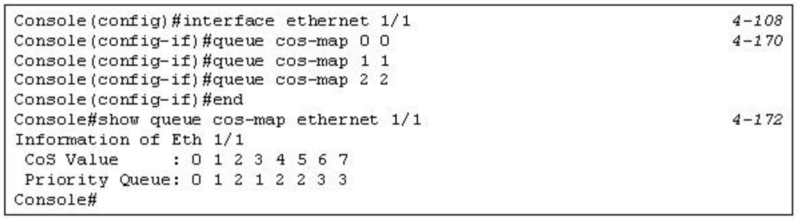
Traffic Classes

Priority	Traffic Class
0	1 (0-3)
1	0 (0-3)
2	0 (0-3)
3	1 (0-3)
4	2 (0-3)
5	2 (0-3)
6	3 (0-3)
7	3 (0-3)

FIG. 156 Web - Traffic Classes

Mapping CoS Values to Egress Queues - CLI

The following example shows how to map CoS values 1 and 2 to CoS priority queue 0, value 0 and 3 to CoS priority queue 1, values 4 and 5 to CoS priority queue 2, and values 6 and 7 to CoS priority queue 3.



```
Console(config)#interface ethernet 1/1                       4-108
Console(config-if)#queue cos-map 0 0                         4-170
Console(config-if)#queue cos-map 1 1
Console(config-if)#queue cos-map 2 2
Console(config-if)#end
Console#show queue cos-map ethernet 1/1                      4-172
Information of Eth 1/1
 CoS Value     : 0 1 2 3 4 5 6 7
 Priority Queue: 0 1 2 1 2 2 3 3
Console#
```

FIG. 157 CLI - Traffic Classes

Mapping specific values for CoS priorities is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

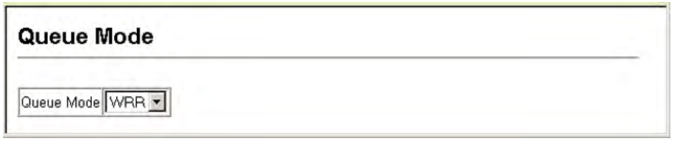
Selecting the Queue Mode

You can set the switch to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before lower priority queues are serviced, or use Weighted Round-Robin (WRR) queuing that specifies a relative weight of each queue. WRR uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.

Command Attributes	
• **WRR:**	Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights 1, 4, 16, 64 for queues 0 through 3 respectively. (This is the default selection.)
• **Strict:**	Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.

Selecting the Queue Mode - Web

Click Priority, Queue Mode. Select Strict or WRR, then click **Apply**.



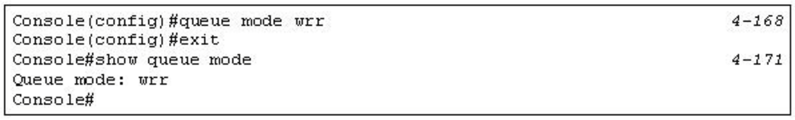
Queue Mode

Queue Mode: WRR

FIG. 158 Web - Selecting the Queue Mode

Selecting the Queue Mode - CLI

The following sets the queue mode to strict priority service mode.



```
Console(config)#queue mode wrr                                    4-168
Console(config)#exit
Console#show queue mode                                           4-171
Queue mode: wrr
Console#
```

FIG. 159 CLI - Selecting the Queue Mode

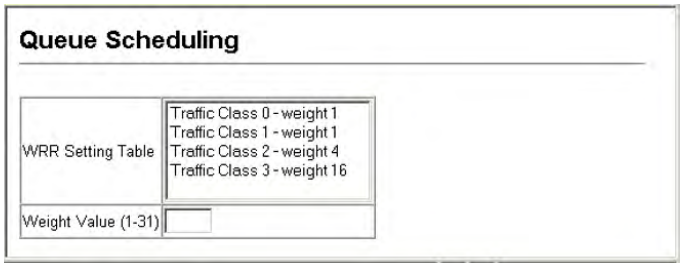
Setting the Service Weight for Traffic Classes

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* section on page 138, the traffic classes are mapped to one of the four egress queues provided for each port. You can assign a weight to each of these queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue will be polled for service, and subsequently affects the response time for software applications assigned a specific priority value.

Command Attributes	
• **WRR Setting Table:**	Displays a list of weights for each traffic class (i.e., queue). • CLI shows Queue ID.
• **Weight Value:**	Set a new weight for the selected traffic class. (Range: 1-255)

Setting the Service Weight for Traffic Classes - Web

Click Priority, Queue Scheduling. Select a traffic class (i.e., output queue), enter a weight, then click **Apply**.



Queue Scheduling

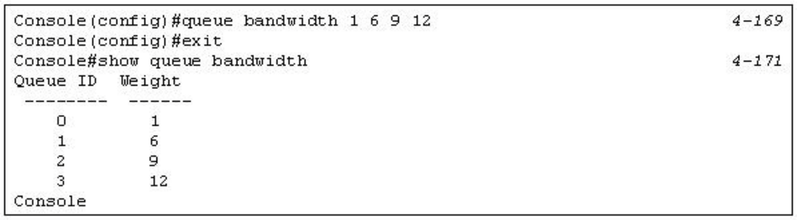
WRR Setting Table:
Traffic Class 0 - weight 1
Traffic Class 1 - weight 1
Traffic Class 2 - weight 4
Traffic Class 3 - weight 16

Weight Value (1-31):

FIG. 160 Web - Configuring Queue Scheduling

Setting the Service Weight for Traffic Classes - CLI

The following example shows how to assign WRR weights of 1, 4, 16 and 64 to the CoS priority queues 0, 1, 2 and 3.



```
Console(config)#queue bandwidth 1 6 9 12                          4-169
Console(config)#exit
Console#show queue bandwidth                                      4-171
Queue ID  Weight
 --------  ------
    0        1
    1        6
    2        9
    3        12
Console
```

FIG. 161 CLI - Configuring Queue Scheduling

Mapping Layer 3/4 Priorities to CoS Values

This 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 IP Port Priority, IP Precedence or DSCP Priority, and then Default Port Priority.
- IP Precedence and DSCP Priority cannot both be enabled. Enabling one of these priority types will automatically disable the other.

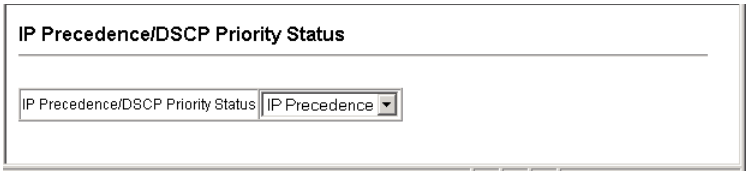
Selecting IP Precedence/DSCP Priority

The switch allows you to choose between using IP Precedence or DSCP priority. Select one of the methods or disable this feature.

Command Attributes	
• Disabled:	Disables both priority services. (This is the default setting.)
• IP Precedence:	Maps layer 3/4 priorities using IP Precedence.
• IP DSCP:	Maps layer 3/4 priorities using Differentiated Services Code Point Mapping.

Selecting IP Precedence/DSCP Priority - Web

Click Priority, IP Precedence/DSCP Priority Status. Select Disabled, IP Precedence or IP DSCP from the scroll-down menu.



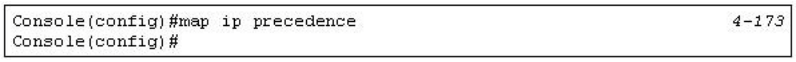
IP Precedence/DSCP Priority Status

IP Precedence/DSCP Priority Status: IP Precedence

FIG. 162 Web - IP Precedence/DSCP Priority Status

Selecting IP Precedence/DSCP Priority - CLI

The following example enables IP Precedence service on the switch.



```
Console(config)#map ip precedence                                4-173
Console(config)#
```

FIG. 163 CLI - IP Precedence/DSCP Priority Status

Mapping 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 default IP Precedence values are mapped one-to-one to Class of Service values (i.e., Precedence value 0 maps to CoS value 0, and so forth). Bits 6 and 7 are used for network control, and the other bits for various application types. ToS bits are defined in the following table.

Mapping IP Precedence			
Priority Level	**Traffic Type**	**Priority Level**	**Traffic Type**
7	Network Control	3	Flash
6	Internetwork Control	2	Immediate
5	Critical	1	Priority
4	Flash Override	0	Routine

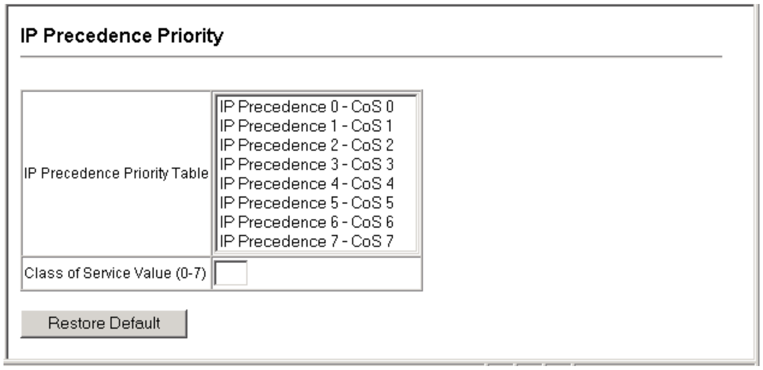
Command Attributes	
• **IP PrecedencePriority Table:**	Shows the IP Precedence to CoS map.
• **Class of Service Value:**	Maps a CoS value to the selected IP Precedence value. Note that “0” represents low priority and “7” represent high priority.

NOTE

IP Precedence settings apply to all interfaces.

Mapping IP Precedence - Web

Click Priority, IP Precedence Priority. Select a port or trunk from the Interface field. Select an entry from the IP Precedence Priority Table, enter a value in the Class of Service Value field, and then click **Apply**.



IP Precedence Priority

IP Precedence Priority Table	IP Precedence 0 - CoS 0 IP Precedence 1 - CoS 1 IP Precedence 2 - CoS 2 IP Precedence 3 - CoS 3 IP Precedence 4 - CoS 4 IP Precedence 5 - CoS 5 IP Precedence 6 - CoS 6 IP Precedence 7 - CoS 7
Class of Service Value (0-7)	

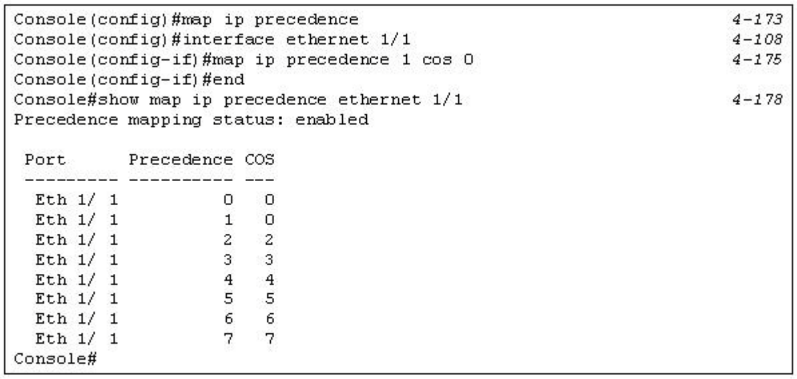
FIG. 164 Web - Mapping IP Precedence Priority Values

NOTE

Mapping specific values for IP Precedence is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Mapping IP Precedence - CLI

The following example globally enables IP Precedence service on the switch, maps IP Precedence value 1 to CoS value 0 on port 5, and then displays all the IP Precedence settings.



```
Console(config)#map ip precedence                                4-173
Console(config)#interface ethernet 1/1                           4-108
Console(config-if)#map ip precedence 1 cos 0                     4-175
Console(config-if)#end
Console#show map ip precedence ethernet 1/1                      4-178
Precedence mapping status: enabled

 Port      Precedence COS
 --------- ---------- ---
  Eth 1/ 1          0   0
  Eth 1/ 1          1   0
  Eth 1/ 1          2   2
  Eth 1/ 1          3   3
  Eth 1/ 1          4   4
  Eth 1/ 1          5   5
  Eth 1/ 1          6   6
  Eth 1/ 1          7   7
Console#
```

FIG. 165 CLI - Mapping IP Precedence Priority Values

NOTE

Mapping specific values for IP Precedence is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Mapping DSCP Priority

The DSCP is six bits wide, allowing coding for up to 64 different forwarding behaviors. The DSCP replaces the ToS bits, and it retains backward compatibility with the three precedence bits so that non-DSCP compliant, ToS-enabled 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 values are defined in the following table. Note that all the DSCP values that are not specified are mapped to CoS value 0.

Mapping DSCP Priority Values	
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

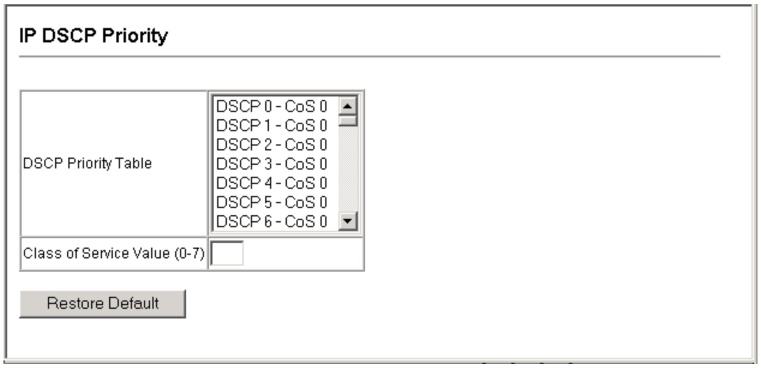
Command Attributes	
• **DSCP Priority Table:**	Shows the DSCP Priority to CoS map.
• **Class of Service Value:**	Maps a CoS value to the selected DSCP Priority value. Note that “0” represents low priority and “7” represent high priority.

NOTE

IP DSCP settings apply to all interfaces.

Mapping DSCP Priority - Web

Click Priority, IP DSCP Priority. Select a port or trunk from the Interface field. Select an entry from the DSCP table, enter a value in the Class of Service Value field, then click **Apply**.



IP DSCP Priority

DSCP Priority Table

DSCP 0 - CoS 0
DSCP 1 - CoS 0
DSCP 2 - CoS 0
DSCP 3 - CoS 0
DSCP 4 - CoS 0
DSCP 5 - CoS 0
DSCP 6 - CoS 0

Class of Service Value (0-7)

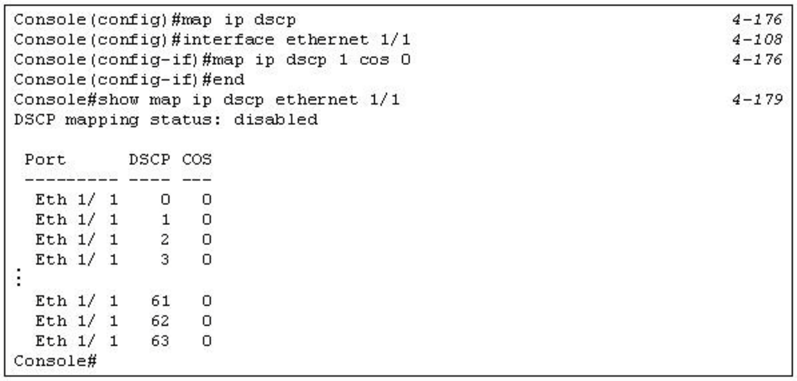
FIG. 166 Web - Mapping IP DSCP Priority Values

NOTE

Mapping specific values for IP Precedence is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Mapping DSCP Priority - CLI

The following example globally enables DSCP Priority service on the switch, maps DSCP value 1 to CoS value 0 on port 5, and then displays all the DSCP Priority settings.



```
Console(config)#map ip dscp                                        4-176
Console(config)#interface ethernet 1/1                             4-108
Console(config-if)#map ip dscp 1 cos 0                             4-176
Console(config-if)#end
Console#show map ip dscp ethernet 1/1                              4-179
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   0
  Eth 1/ 1   62   0
  Eth 1/ 1   63   0
Console#
```

FIG. 167 CLI - Mapping IP DSCP Priority Values

NOTE

Mapping specific values for IP Precedence is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Mapping IP Port Priority

You can also map network applications to Class of Service values based on the IP port number (i.e., TCP/UDP port number) in the frame header.

Some of the more common TCP service ports include: HTTP: 80, FTP: 21, Telnet: 23 and POP3: 110.

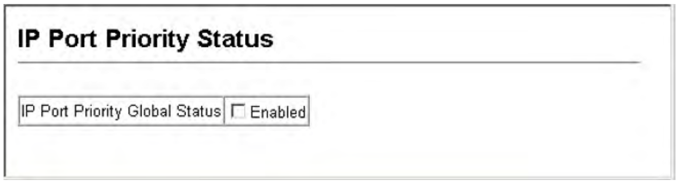
Command Attributes	
• **IP Port Priority Status:**	Enables or disables the IP port priority.
• **Interface:**	Selects the port or trunk interface to which the settings apply.
• **IP Port Priority Table:**	Shows the IP port to CoS map.
• **IP Port Number (TCP/UDP):**	Set a new IP port number.
• **Class of Service Value:**	Sets a CoS value for a new IP port. Note that “0” represents low priority and “7” represent high priority.

NOTE

IP Port Priority settings apply to all interfaces.

Mapping IP Port Priority - Web

Click Priority, IP Port Status. Set IP Port Priority Status to Enabled.

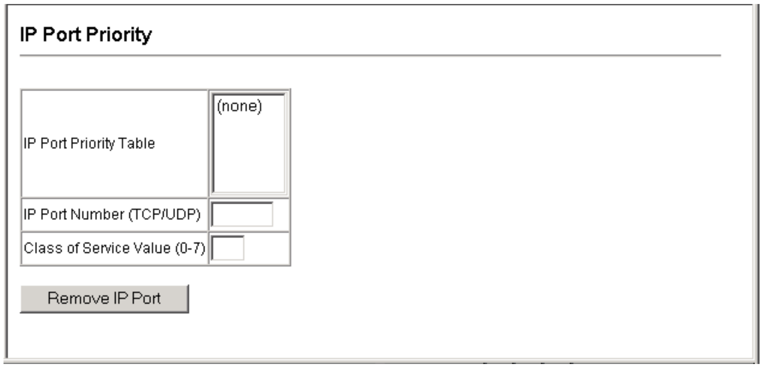


IP Port Priority Status

IP Port Priority Global Status ☐ Enabled

FIG. 168 Web - Enabling IP Port Priority Status

Click Priority, IP Port Priority. Select a port or trunk from the Interface field. Enter the port number for a network application in the IP Port Number box and the new CoS value in the Class of Service box, and then click Add IP Port.



IP Port Priority

IP Port Priority Table	(none)
IP Port Number (TCP/UDP)	
Class of Service Value (0-7)	

Remove IP Port

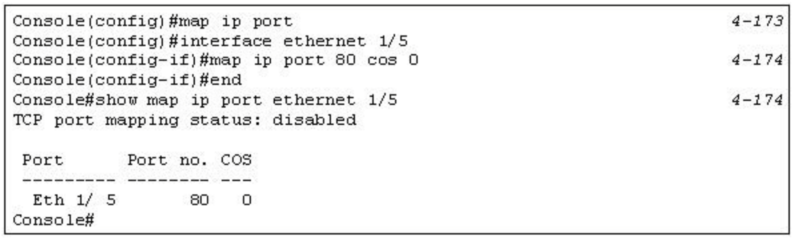
FIG. 169 Web - Mapping IP Port Priority

NOTE

Mapping specific values for IP Precedence is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Mapping IP Port Priority - CLI

The following example globally enables IP Port Priority service on the switch, maps HTTP traffic on port 5 to CoS value 0, and then displays all the IP Port Priority settings for that port.



```
Console(config)#map ip port                                       4-173
Console(config)#interface ethernet 1/5
Console(config-if)#map ip port 80 cos 0                           4-174
Console(config-if)#end
Console#show map ip port ethernet 1/5                             4-174
TCP port mapping status: disabled

 Port      Port no. COS
 --------- -------- ---
  Eth 1/ 5       80   0
Console#
```

FIG. 170 Web - Mapping IP Port Priority

NOTE

Mapping specific values for IP Precedence is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

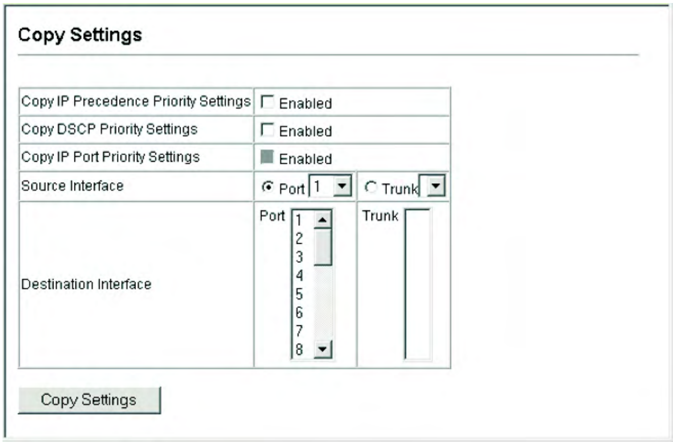
Copy Settings

Use the Copy Settings page to copy IP Precedence Priority Settings, DSCP Priority Settings, and IP Port Priority Settings from a source port or trunk to a destination port or trunk.

Command Attributes	
• **Copy IP Precedence Priority Settings:**	Enables or disables copying IP Precedence Priority settings.
• **Copy DSCP Priority Settings:**	Enables or disables copying DSCP Priority settings.
• **Copy IP Port Priority Settings:**	Enables or disables copying IP Port Priority settings.
• **Source Interface:**	Specifies the port or trunk to copy settings from.
• **Destination Interface:**	Specifies the ports or trunks to copy settings to.
• **Copy Settings:**	Carries out the command.

Copy Settings - Web

Click Priority, Copy Settings. Select the source priority settings to be copied, enter the source port or trunk number and choose the destination interface/s to copy to, then select **Copy Settings**.



Copy Settings

Copy IP Precedence Priority Settings	□ Enabled	
Copy DSCP Priority Settings	□ Enabled	
Copy IP Port Priority Settings	▨ Enabled	
Source Interface	● Port 1 ▾	○ Trunk ▾
Destination Interface	Port 1 2 3 4 5 6 7 8	Trunk

FIG. 171 Web - Copy Settings

Copy Settings - CLI

CLI – The following example shows how to map HTTP traffic to CoS value 0 on port 5, maps IP precedence to CoS 0 to port 6, and enables mapping IP DSCP globally.

```
Console#con
Console(config)#interface ethernet 1/5
Console(config-if)#map ip port 80 cos 0 360
Console(config)#interface ethernet 1/6
Console(config-if)#map ip precedence 1 cos 0 361
Console(config-if)#exit
Console(config)#map ip dscp 362
Console(config)#
```

Mapping CoS Values to ACLs

Use the ACL CoS Mapping page to set the output queue for packets matching an ACL rule as shown in the following table. Note that the specified CoS value is only used to map the matching packet to an output queue; it is not written to the packet itself. For information on mapping the CoS values to output queues, see page 138.

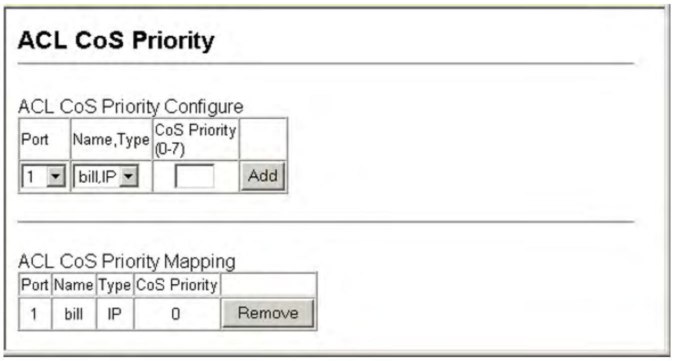
CoS to ACL Mapping				
Queue	0	1	2	3
Priority	1,2	0,3	4,5	6,7

Command Usage - You must configure an ACL mask before you can map CoS values to the rule.

Command Attributes	
• **Port:**	Selects the port to which the ACL CoS is configured on.
• **Name:**	Name of ACL. For information on configuring ACLs, see the *Configuring ACLs* section on page 73.
• **Type:**	Type of ACL (IP or MAC).
• **CoS Priority:**	Enables the CoS priority value level.
• **Add:**	Adds the specified information to the port.
• **ACL CoS Priority Mapping:**	Displays the configured information.

Mapping CoS Values to ACLs - Web

Click Priority, ACL CoS Priority. Select a port, select an ACL rule, specify a CoS priority, then click **Add**.



ACL CoS Priority

ACL CoS Priority Configure

Port	Name,Type	CoS Priority (0-7)	
1 ▾	bill,IP ▾		Add

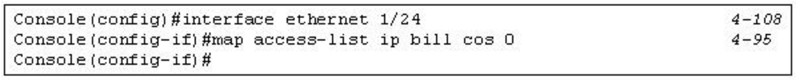
ACL CoS Priority Mapping

Port	Name	Type	CoS Priority	
1	bill	IP	0	Remove

FIG. 172 Web - ACL CoS Priority

Mapping CoS Values to ACLs - CLI

This example assigns a CoS value of zero to packets matching rules within the specified ACL on port 1.



```
Console(config)#interface ethernet 1/24                          4-108
Console(config-if)#map access-list ip bill cos 0                 4-95
Console(config-if)#
```

FIG. 173 CLI - ACL CoS Priority

Changing Priorities Based on ACL Rules

You can change traffic priorities for frames matching the defined ACL rule. (This feature is commonly referred to as ACL packet marking.) This switch can change the IEEE 802.1p priority, IP Precedence, or DSCP Priority of IP frames; or change the IEEE 802.1p priority of Layer 2 frames. (This feature is commonly referred to as ACL packet marking.) Use the no form to remove the ACL marker.

Command Usage

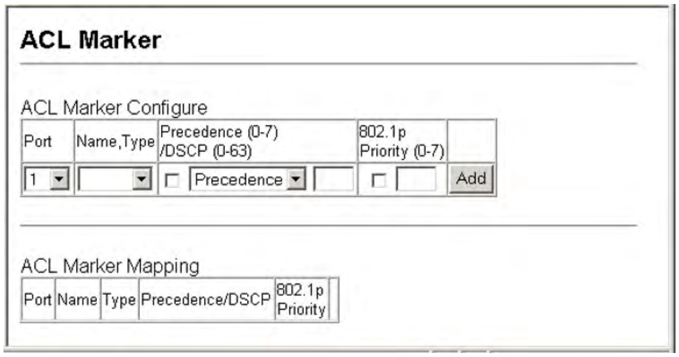
- You must configure an ACL mask before you can change priorities based on a rule.
- Traffic priorities may be included in the IEEE 802.1p priority tag. This tag is also incorporated as part of the overall IEEE 802.1Q VLAN tag. The 802.1p priority may be set for either Layer 2 or IP frames.
- The IP frame header also includes priority bits in the Type of Service (ToS) octet. The Type of Service octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. Note that the IP frame header can include either the IP Precedence or DSCP priority type.
- The precedence for priority mapping by this switch is IP Precedence or DSCP Priority, and then 802.1p priority.

Command Attributes	
• **Port:**	Port identifier.
• **Name:**	Name of ACL.
• **Type:**	Type of ACL (IP or MAC).
• **Precedence:**	IP Precedence value. (Range: 0-7)
• **DSCP:**	Differentiated Services Code Point value. (Range: 0-63)
• **802.1p Priority:**	Class of Service value in the IEEE 802.1p priority tag. (Range: 0-7; 7 is the highest priority)

Changing Priorities Based on ACL Rules - Web

Click Priority, ACL Marker. Select a port and an ACL rule.

- To specify a ToS priority, mark the Precedence/DSCP check box, select Precedence or DSCP from the scroll-down box, and enter a priority.
- To specify an 802.1p priority, mark the 802.1p Priority check box, and enter a priority. Then click Add.



ACL Marker

ACL Marker Configure

Port	Name,Type	Precedence (0-7) /DSCP (0-63)	802.1p Priority (0-7)	
1 ▾	▾	□ Precedence ▾	□	Add

ACL Marker Mapping

Port	Name	Type	Precedence/DSCP	802.1p Priority

FIG. 174 Changing Priorities Based on ACL Rules

Changing Priorities Based on ACL Rules - CLI

This example changes the DSCP priority for packets matching an IP ACL rule, and the 802.1p priority for packets matching a MAC ACL rule.

```
Console(config)#interface ethernet 1/1300
Console(config-if)#match access-list ip bill set dscp 0275
Console(config-if)#match access-list mac mike set priority 0286
Console(config-if)#end
Console#show marking276
Interface ethernet 1/1
 match access-list IP bill set DSCP 0
 match access-list MAC a set priority 0
Console#
```

Multicast Filtering

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 the hosts which subscribed to this service.

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 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. This procedure is called multicast filtering.

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).

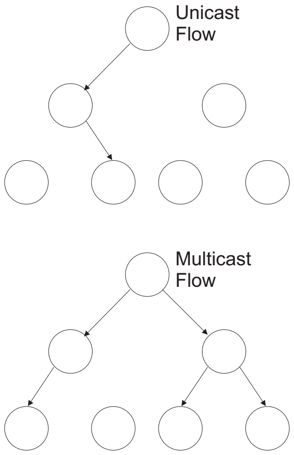


FIG. 175 Unicast Flow vs. Multicast Flow

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 to monitor IGMP service requests passing between multicast clients and servers, and dynamically configure the switch ports which need to forward multicast traffic.

- **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 (see the *Specifying Interfaces Attached to a Multicast Router* section on page 152). 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.
- **Static IGMP Host Interface** – For multicast applications that you need to control more carefully, you can manually assign a multicast service to specific interfaces on the switch (see the *Assigning Ports to Multicast Services* section on page 153).

Configuring IGMP Snooping and Query Parameters

You can configure the switch to forward multicast traffic intelligently. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.

NOTE

Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

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 multicast filters accordingly.
- **IGMP Query** – 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 adjacent multicast switch/router to ensure that it will continue to receive the multicast service.

Command Attributes	
• IGMP Status:	When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. • This is also 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. • Default: Enabled
• IGMP Query Count:	Sets the maximum number of queries issued for which there has been no response before the switch takes action to solicit reports. • Default: 2 • Range: 2 - 10
• IGMP Query Interval:	Sets the frequency of time at which the switch sends IGMP host-query messages. • Default: 125 secs. • Range: 60 - 125 secs.
• IGMP Report Delay:	Sets the time (in seconds) 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. • Default: 10 • Range: 5-30
• Query Timeout:	Sets the time (in seconds) the switch waits after the previous querier has stopped querying before it takes over as the querier. • Default: 300 seconds • Range: 300 - 500
• IGMP Version:	Sets the protocol version for compatibility with other devices on the network. • Default: 2 • Range: 1 - 2

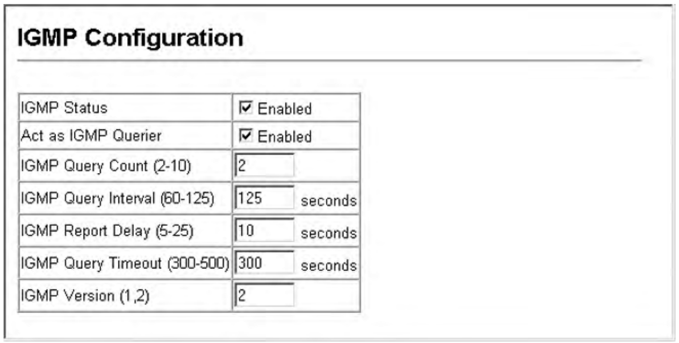
NOTE

1. *All systems on the subnet must support the same version.*
2. *Some attributes are only enabled for IGMPv2, including IGMP Report Delay and IGMP Query Timeout.*

Configuring IGMP Snooping and Query Parameters - Web

Click IGMP, IGMP Configuration. Adjust the IGMP settings as required, and then click **Apply**.

The default settings are shown below.



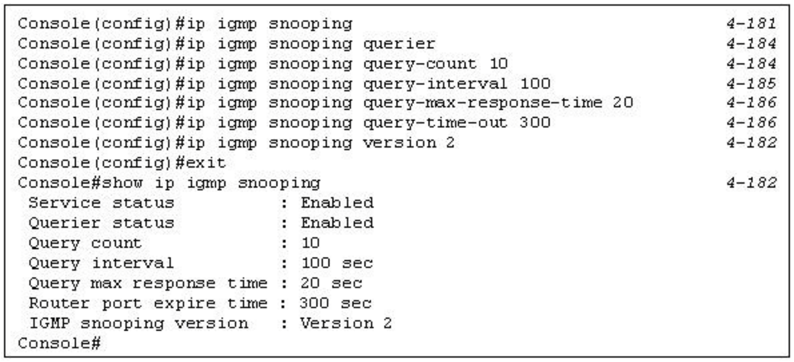
IGMP Configuration

IGMP Status	☑ Enabled
Act as IGMP Querier	☑ Enabled
IGMP Query Count (2-10)	2
IGMP Query Interval (60-125)	125 seconds
IGMP Report Delay (5-25)	10 seconds
IGMP Query Timeout (300-500)	300 seconds
IGMP Version (1,2)	2

FIG. 176 Web - IGMP Configuration

Configuring IGMP Snooping and Query Parameters - CLI

This example modifies the settings for multicast filtering, and then displays the current status.



```
Console(config)#ip igmp snooping                                    4-181
Console(config)#ip igmp snooping querier                            4-184
Console(config)#ip igmp snooping query-count 10                     4-184
Console(config)#ip igmp snooping query-interval 100                 4-185
Console(config)#ip igmp snooping query-max-response-time 20         4-186
Console(config)#ip igmp snooping query-time-out 300                 4-186
Console(config)#ip igmp snooping version 2                          4-182
Console(config)#exit
Console#show ip igmp snooping                                       4-182
 Service status          : Enabled
 Querier status          : Enabled
 Query count             : 10
 Query interval          : 100 sec
 Query max response time : 20 sec
 Router port expire time : 300 sec
 IGMP snooping version   : Version 2
Console#
```

FIG. 177 CLI - IGMP Configuration

Displaying Interfaces Attached to a Multicast Router

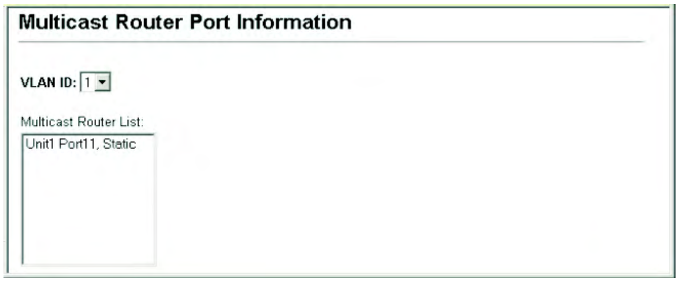
Multicast routers that are attached to ports on the switch use information obtained from IGMP, along with a multicast routing protocol such as DVMRP, to support IP multicasting across the Internet. These routers may be dynamically discovered by the switch or statically assigned to an interface on the switch.

You can use the Multicast Router Port Information page to display the ports on this switch attached to a neighboring multicast router/switch for each VLAN ID.

Command Attributes	
• **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.

Displaying Interfaces Attached to a Multicast Router - Web

Click IGMP, Multicast Router Port Information. Select the required VLAN ID from the scroll-down list to display the associated multicast routers.



Multicast Router Port Information

VLAN ID: 1

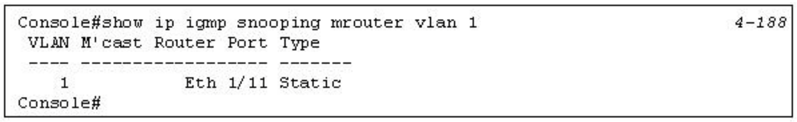
Multicast Router List:

Unit1 Port11, Static

FIG. 178 Web - Displaying Multicast Router Port Information

Displaying Interfaces Attached to a Multicast Router - CLI

This example shows that Port 11 has been statically configured as a port attached to a multicast router.



```
Console#show ip igmp snooping mrouter vlan 1                          4-188
 VLAN M'cast Router Port Type
 ---- ------------------ -------
    1           Eth 1/11 Static
Console#
```

FIG. 179 Web - Displaying Multicast Router Port Information

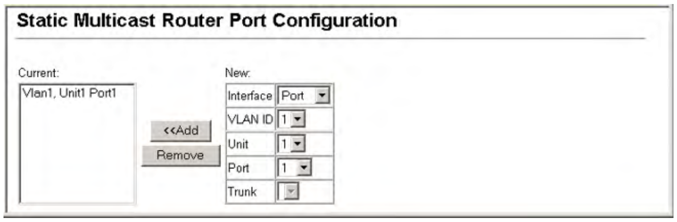
Specifying Interfaces Attached to a Multicast Router

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/switch connected over the network to an interface (port or trunk) on your switch, you can manually configure that interface to join all the current multicast groups. This can ensure that multicast traffic is passed to all the appropriate interfaces within the switch.

Command Attributes	
• **Interface:**	Activates the Port or Trunk scroll down list.
• **VLAN ID:**	Selects the VLAN to propagate all multicast traffic coming from the attached multicast router/ switch.
• **Port** or **Trunk:**	Specifies the interface attached to a multicast router.

Specifying Interfaces Attached to a Multicast Router - Web

Click IGMP, Static Multicast Router Port Configuration. Specify the interfaces attached to a multicast router, indicate the VLAN which will forward all the corresponding multicast traffic, and then click **Add**. After you have completed adding interfaces to the list, click **Apply**.



Static Multicast Router Port Configuration

Current:

Vlan1, Unit1 Port1

New:

Interface: Port

VLAN ID: 1

Unit: 1

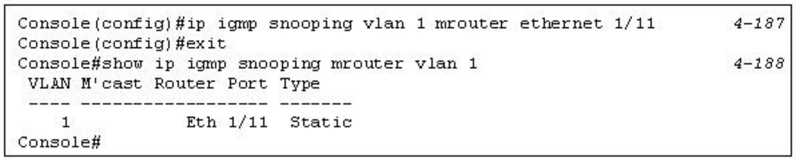
Port: 1

Trunk:

FIG. 180 Web - Static Multicast Router Port Configuration

Specifying Interfaces Attached to a Multicast Router - CLI

This example configures port 11 as a multicast router port within VLAN 1.



```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11        4-187
Console(config)#exit
Console#show ip igmp snooping mrouter vlan 1                          4-188
 VLAN M'cast Router Port Type
 ---- ------------------ -------
    1            Eth 1/11  Static
Console#
```

FIG. 181 CLI - Static Multicast Router Port Configuration

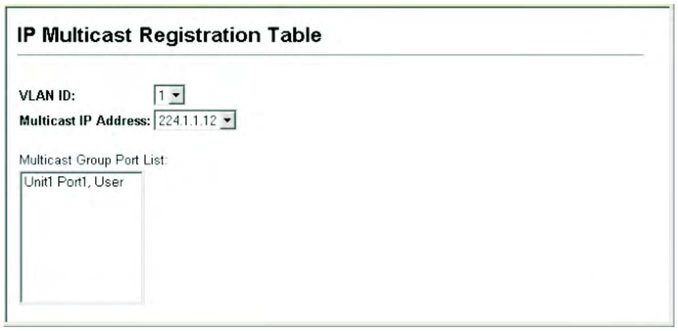
Displaying Port Members of Multicast Services

You can display the port members associated with a specified VLAN and multicast IP address.

Command Attributes	
• **VLAN ID:**	Selects the VLAN in which to display port members.
• **Multicast IP Address:**	The IP address for a specific multicast service
• **Multicast Group Port List:**	Ports propagating a multicast service; i.e., ports that belong to the indicated VLAN group.

Displaying Port Members of Multicast Services - Web

Click IGMP, IP Multicast Registration Table. Select the VLAN ID and the IP address for a multicast service. The switch will display all the ports that are propagating this multicast service.



IP Multicast Registration Table

VLAN ID: 1

Multicast IP Address: 224.1.1.12

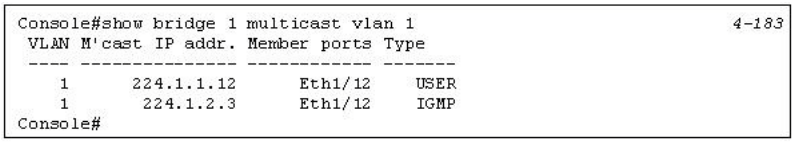
Multicast Group Port List:

Unit1 Port1, User

FIG. 182 Web - IP Multicast Registration Table

Displaying Port Members of Multicast Services - CLI

This example displays all the known multicast services supported on VLAN 1, along with the ports propagating the corresponding services. The type field shows if this entry was learned dynamically or was statically configured.



```
Console#show bridge 1 multicast vlan 1                               4-183
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1      224.1.1.12      Eth1/12     USER
    1       224.1.2.3      Eth1/12     IGMP
Console#
```

FIG. 183 CLI - IP Multicast Registration Table

Assigning Ports to Multicast Services

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages as described in *Configuring IGMP Snooping and Query Parameters* section on page 150. For certain applications that require tighter control, you may need 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.

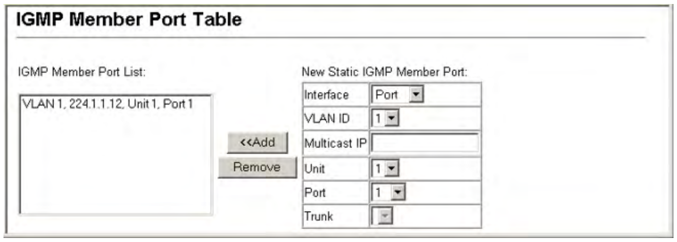
Command Usage

- Static multicast addresses are never aged out.
- When a multicast address is assigned to specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

Command Attributes	
• **Interface:**	Activates the Port or Trunk scroll down list.
• **VLAN ID:**	Selects the VLAN to propagate all multicast traffic coming from the attached multicast router/ switch.
• **Multicast IP:**	The IP address for a specific multicast service.
• **Port** or **Trunk:**	Specifies the interface attached to a multicast router.

Assigning Ports to Multicast Services - Web

Click IGMP, IGMP Member Port Table. Specify the interface attached to a multicast service (via an IGMP-enabled switch or multicast router), indicate the VLAN that will propagate the multicast service, specify the multicast IP address, and then click **Add**. After you have completed adding ports to the member list, click **Apply**.



IGMP Member Port Table

IGMP Member Port List:

VLAN 1, 224.1.1.12, Unit 1, Port 1

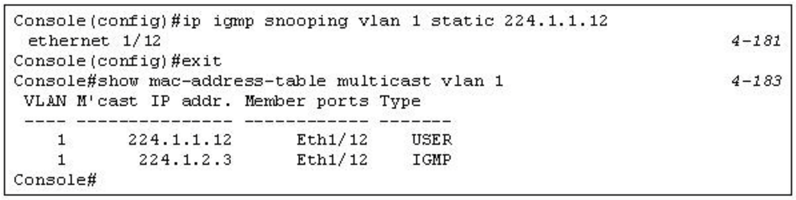
New Static IGMP Member Port:

Interface	Port
VLAN ID	1
Multicast IP	
Unit	1
Port	1
Trunk	

FIG. 184 Web - IGMP Member Port Table

Assigning Ports to Multicast Services - CLI

This example assigns a multicast address to VLAN 1, and then displays all the known multicast services supported on VLAN 1.



```
Console(config)#ip igmp snooping vlan 1 static 224.1.1.12
 ethernet 1/12                                                       4-181
Console(config)#exit
Console#show mac-address-table multicast vlan 1                      4-183
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1      224.1.1.12      Eth1/12     USER
    1       224.1.2.3      Eth1/12     IGMP
Console#
```

FIG. 185 CLI - IGMP Member Port Table

Configuring Domain Name Service

Overview

The Domain Naming System (DNS) service 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 Server Parameters

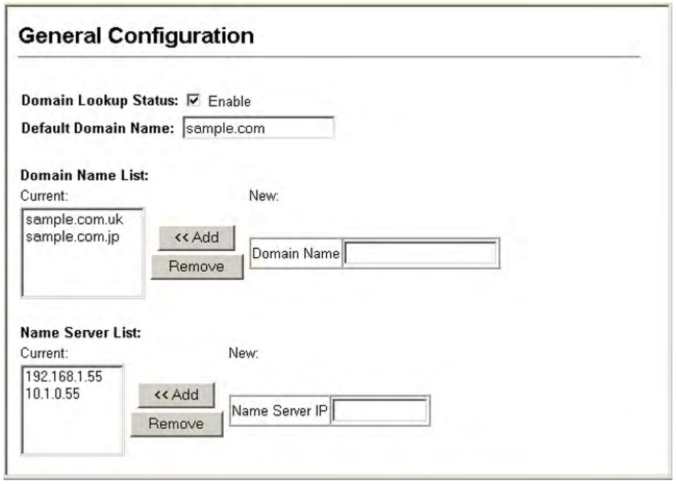
Command Usage

- 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 default domain name is not used.
- When an incomplete host name is received by the DNS server 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.

Command Attributes	
• Domain Lookup Status:	Enables DNS host name-to-address translation.
• Default Domain Name:	Defines the default domain name appended to incomplete host names. • Range: 1-64 alphanumeric characters • Do not include the initial dot that separates the host name from the domain name.
• Domain Name List:	Defines define a list of domain names that can be appended to incomplete host names. • Range: 1-64 alphanumeric characters. 1-5 names • Do not include the initial dot that separates the host name from the domain name.
• 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

Configuring General DNS Server Parameters - Web

Select DNS, General Configuration. Set the default domain name or list of domain names, specify one or more name servers to use for address resolution, enable domain lookup status, and click **Apply**.



General Configuration

Domain Lookup Status: ☑ Enable

Default Domain Name: sample.com

Domain Name List:

Current:
sample.com.uk
sample.com.jp

New: Domain Name

Name Server List:

Current:
192.168.1.55
10.1.0.55

New: Name Server IP

FIG. 186 Configuring DNS

Configuring General DNS Server Parameters - CLI

This example sets a default domain name and a domain list. However, remember that if a domain list is specified, the default domain name is not used.

```
Console(config)#ip domain-name sample.com380
Console(config)#ip domain-list sample.com.uk381
Console(config)#ip domain-list sample.com.jp
Console(config)#ip name-server 192.168.1.55 10.1.0.55382
Console(config)#ip domain-lookup383
Console#show dns384
Domain Lookup Status:
    DNS enabled
Default Domain Name:
    .sample.com
Domain Name List:
    .sample.com.uk
    .sample.com.jp
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

Configuring Static DNS Host to Address Entries

You can manually configure static entries in the DNS table that are used to map domain names to IP addresses.

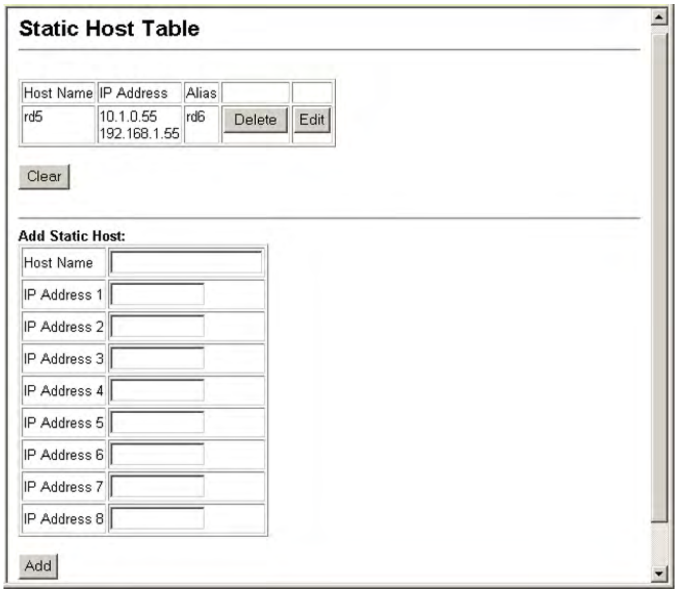
Command Usage

- 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.

Field Attributes	
• **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
• **Alias:**	Displays the host names that are mapped to the same address(es) as a previously configured entry.

Configuring Static DNS Host to Address Entries - Web

Select DNS, Static Host Table. Enter a host name and one or more corresponding addresses, then click **Apply**.



Static Host Table

Host Name	IP Address	Alias		
rd5	10.1.0.55 192.168.1.55	rd6	Delete	Edit

Add Static Host:

Host Name	
IP Address 1	
IP Address 2	
IP Address 3	
IP Address 4	
IP Address 5	
IP Address 6	
IP Address 7	
IP Address 8	

FIG. 187 Web - Mapping IP Addresses to a Host Name

Configuring Static DNS Host to Address Entries - CLI

This example maps two address to a host name, and then configures an alias host name for the same addresses.

```
Console(config)#ip host rd5 192.168.1.55 10.1.0.55379
Console(config)#ip host rd6 10.1.0.55379
Console#show host384

Hostname
 rd5
Inet address
 10.1.0.55 192.168.1.55
Alias
 1.rd6
```

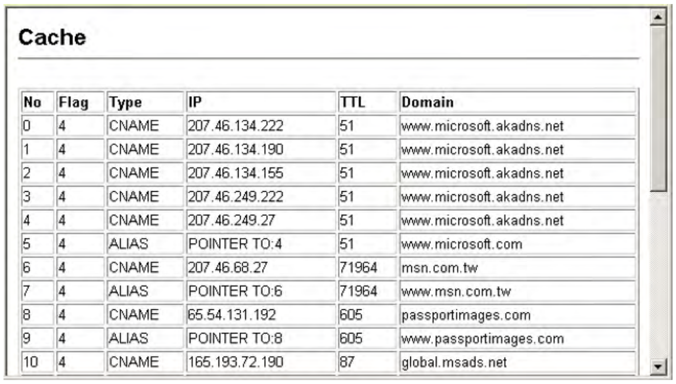
Displaying the DNS Cache

You can display entries in the DNS cache that have been learned via the designated name servers.

Field Attributes	
• **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 canonical or primary name for the owner, and ALIAS which specifies multiple domain names 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.

Displaying the DNS Cache - Web

Select DNS, Cache.



Cache

No	Flag	Type	IP	TTL	Domain
0	4	CNAME	207.46.134.222	51	www.microsoft.akadns.net
1	4	CNAME	207.46.134.190	51	www.microsoft.akadns.net
2	4	CNAME	207.46.134.155	51	www.microsoft.akadns.net
3	4	CNAME	207.46.249.222	51	www.microsoft.akadns.net
4	4	CNAME	207.46.249.27	51	www.microsoft.akadns.net
5	4	ALIAS	POINTER TO:4	51	www.microsoft.com
6	4	CNAME	207.46.68.27	71964	msn.com.tw
7	4	ALIAS	POINTER TO:6	71964	www.msn.com.tw
8	4	CNAME	65.54.131.192	605	passportimages.com
9	4	ALIAS	POINTER TO:8	605	www.passportimages.com
10	4	CNAME	165.193.72.190	87	global.msads.net

FIG. 188 Web - Displaying the DNS Cache

Displaying the DNS Cache - CLI

This example displays all the resource records learned from the designated name servers.

```
Console#show dns cache384
NO       FLAG     TYPE     IP               TTL      DOMAIN
0         4       CNAME    207.46.134.222   51       www.microsoft.akadns.net
1         4       CNAME    207.46.134.190   51       www.microsoft.akadns.net
2         4       CNAME    207.46.134.155   51       www.microsoft.akadns.net
3         4       CNAME    207.46.249.222   51       www.microsoft.akadns.net
4         4       CNAME    207.46.249.27    51       www.microsoft.akadns.net
5         4       ALIAS    POINTER TO:4     51       www.microsoft.com
6         4       CNAME    207.46.68.27     71964    msn.com.tw
7         4       ALIAS    POINTER TO:6     71964    www.msn.com.tw
8         4       CNAME    65.54.131.192    605      passportimages.com
9         4       ALIAS    POINTER TO:8     605      www.passportimages.com
10        4       CNAME    165.193.72.190   87       global.msads.net
Console#
```

CLI (Command Line Interface)

Overview

This chapter describes how to use the Command Line Interface (CLI).

Using the Command Line Interface

When accessing the management interface for the switch over a direct connection to the server's console port, or via a Telnet connection, 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.

CAUTION

When ES3526V 24 Port Fast Ethernet switches are stacked together, you must connect to the RS-232 port on the Master unit to be able to access the CLI.

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 name is "**Admin**" and the password is "**1988**")
   - 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 Intelligent Fast Ethernet PoE Switch 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).

CAUTION

The IP address for this switch is unassigned by default.

To access the switch through a Telnet session, you must first set the IP address for the switch, 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 10.1.0.1 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
```

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-0#” prompt for the administrator to show that you are using privileged access mode (i.e., Privileged Exec), or “Vty-0>” for the guest to show that you are using normal access mode (i.e., Normal Exec).
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 Intelligent Fast Ethernet PoE Switch is opened.
      To end the CLI session, enter [Exit].

Console#
```

CAUTION

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 for the current command class (Normal Exec or Privileged Exec) or configuration class (Global, ACL, Interface, Line, or VLAN Database). You can also display a list of valid keywords for a specific command. For example, the command “**show ?**” displays a list of possible show commands:

```
Console#show ?
  access-group       Access groups
  access-list        Access lists
  bridge-ext         Bridge extend information
  calendar           Date information
  dot1x              Show 802.1x content
  garp               Garp property
  gvrp               Show gvrp information of interface
  history            Information of history
  hosts              Host information
  interfaces         Information of interfaces
  ip                 IP information
  lacp               LACP statistics
  line               TTY line information
  log                Login records
  logging            Show the contents of logging buffers
  mac                MAC access lists
  mac-address-table  Set configuration of the address table
  management         Management IP filter
  map                Map priority
  marking            Specify marker
  port               Characteristics of the port
  power              Show power
  public-key         Public key information
  queue              Information of priority queue
  radius-server      Radius server information
  running-config     The system configuration of running
  snmp               SNMP statistics
  sntp               Sntp
  spanning-tree      Specify spanning-tree
  ssh                Secure shell
  startup-config     The system configuration of starting up
  system             Information of system
  tacacs-server      Login by tacacs server
  users              Display information about terminal lines
  version            System hardware and software status
  vlan               Switch VLAN Virtual Interface
Console#show
```

The command “**show interfaces ?**” will display the following information:

```
Console>show interfaces ?
  counters    Interface counters information
  status      Interface status information
  switchport  Interface switchport information
```

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?
snmp            sntp           spanning-tree   ssh          startup-config  system
```

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:

Command Modes

Class	**Mode**	
Exec	Normal Privileged	
Configuration	Global*	Access Control List Interface Line VLAN Database

* You must be in Privileged Exec mode to access any of the configuration modes.

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" (see page 169).

To enter Privileged Exec mode, enter the following commands and passwords:

```
Username: Admin
Password: [system login password]

      CLI session with the Intelligent Fast Ethernet PoE Switch is opened.
      To end the CLI session, enter [Exit].

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 nonvolatile storage, use the **copy running-config startup-config** command.

The configuration commands are organized into different modes:

- **Global Configuration** - These commands modify the system level configuration, and include commands such as *hostname* and *snmp-server community.*
- **Access Control List Configuration** - These commands are used for packet filtering.
- **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 commands such as *parity* and *databits*.
- **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.

Configuration Commands			
Mode	**Command**	**Prompt**	**Page**
Line	line {console | vty}	Console(config-line)#	165

Access Control List	access-list ip standard
	access-list ip extended
	access-list ip mask-precedence
	access-list mac
	access-list mac mask-precedence
		Console(config-std-acl)
		Console(config-ext-acl)
		Console(config-ip-mask-acl)
		Console(config-mac-acl)
		Console(config-mac-mask-acl)
			209

Interface	interface {ethernet *port* | port-channel *id*| vlan *id*}	Console(config-if)#	231
VLAN	vlan database	Console(config-vlan)	255

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:

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.

Keystroke Commands (Cont.)	
Keystroke	**Function**
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-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.

Command Groups

The system commands can be broken down into the functional groups shown below.

Command Group Index		
Command Group	**Description**	**Page #**
• **Line**	Sets communication parameters for the serial port and Telnet, including baud rate and console time-out	165
• **General**	Basic commands for entering privileged access mode, restarting the system, or quitting the CLI	169
• **System Management**	Controls system logs, system passwords, user name, browser management options, and a variety of other system information	171
• **Flash/File**	Manages code image or switch configuration files	193
• **Power over Ethernet**	Configures power output for connect devices	196
• **Authentication**	Configures RADIUS and TACACS+ client-server authentication for logon access and commands for IEEE 802.1x port access control.	199
• **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)	209
• **SNMP**	Activates authentication failure traps; configures community access strings, and trap managers; also configures IP address filtering	224
• **Interface**	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs	231
• **Mirror Port**	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port	237
• **Rate Limiting**	Controls the maximum rate for traffic transmitted or received on a port	238
• **Link Aggregation**	Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks	239
• **Address Table**	Configures the address table for filtering specified addresses, displays current entries, clears the table, or sets the aging time	246
• **Spanning Tree**	Configures Spanning Tree settings for the switch	248
• **VLANs**	Configures VLAN settings, and defines port membership for VLAN groups; also enables or configures private VLANs	255
• **GVRP and Bridge Extension**	Configures GVRP settings that permit automatic VLAN learning; shows the configuration for bridge extension MIB	262

Command Group Index (Cont.)		
Command Group	**Description**	**Page**
• Priority	Sets port priority for untagged frames, relative weight for each priority queue, also sets priority for TCP/UDP traffic types, IP precedence, and DSCP	264
• Multicast Filtering	Configures IGMP multicast filtering, query parameters, and specifies ports attached to a multicast router	271
• IP Interface	Configures the IP address and gateway for management access	275
• DNS	Configures DNS services	278

Line Commands

You can access the onboard configuration program by attaching a VT100 compatible device to the switch's serial port. These commands are used to set communication parameters for the serial port or Telnet (i.e., a virtual terminal).

Line Commands	
Command	**Function**

line
Use this command to identify 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)#`

login
Use this command to enable 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/TACACS software installed on those servers.
	Example:
	`Console(config-line)#login local`
	`Console(config-line)#`

Line Commands (Cont.)	
Command	**Function**

password
Use this command to specify 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: 8 characters plain text, 32 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)#`

timeout login response
Use this command to set 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 number of seconds.
	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)#`

exec-timeout
Use this command to set 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 number of seconds.
	Range: 0 - 65535 seconds; 0: no timeout
	Default Setting: CLI and Telnet: 600 seconds (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)#`

Line Commands (Cont.)	
Command	**Function**

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.
	• This command applies to both the local console and Telnet connections.
	Example: To set the password threshold to five attempts, enter this command:
	`Console(config-line)#password-thresh 5`
	`Console(config-line)#`

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: no silent-time
	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)#`
	***Note**: This command applies only to the serial port.*

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)#`
	***Note**: This command applies only to the serial port.*

Line Commands (Cont.)

Command	**Function**

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)#`
	***Note**: This command applies only to the serial port.*

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, 57600, 115200 bps)
	Default Setting: 9600
	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 57600 bps, enter this command:
	`Console(config-line)#speed 57600`
	`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}`
	• 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)#`
	***Note**: This command applies only to the serial port.*

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#`

<table>
<tr><th colspan="2">Line Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Function</th></tr>
<tr><td>

show line

This command displays the terminal line’s parameters.

</td><td>

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
  Interactive timeout: Disabled
  Login timeout:       Disabled
  Silent time:         Disabled
  Baudrate:            9600
  Databits:            8
  Parity:              none
  Stopbits:            1

 VTY configuration:
  Password threshold:  3 times
  Interactive timeout: 600 sec
  Login timeout:       300 sec
console#
```

</td></tr>
</table>

General Commands

<table>
<tr><th colspan="2">General Commands</th></tr>
<tr><th>Command</th><th>Function</th></tr>
<tr><td>

enable

This command activates *Privileged Exec* mode.

</td><td>

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#
```

In privileged mode, additional commands are available, and certain commands display additional information. See the *Understanding Command Modes* section on page 162.

</td></tr>
<tr><td>

disable

This command returns to *Normal Exec* mode from privileged mode.

</td><td>

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
```

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 the *Understanding Command Modes* section on page 162.

</td></tr>
</table>

General Commands (Cont.)

Command	Function

configure
This command activates *Global Configuration* mode.
You must enter this mode to modify any settings on the switch.
	Default Setting: None
	Command Mode: Privileged Exec
	Example:
	`Console#configure`
	`Console(config)#`
	You must also enter Global Configuration mode prior to enabling some of the other configuration modes, including Interface Configuration, Line Configuration, and VLAN Database Configuration. See the *Understanding Command Modes* section on page 162.

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)#`

reload
This command restarts the system.
	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`
	`System will be restarted, continue <y/n>? y`
	***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.*

end
This command returns to Privileged Exec mode.
	Default Setting: None
	Command Mode: Global Configuration, Interface Configuration, Line Configuration, and VLAN Database Configuration.
	Example: This example shows how to return to the Privileged Exec mode from the Interface Configuration mode:
	`Console(config-if)#end`
	`Console#`

General Commands (Cont.)

Command	**Function**

exit
This command returns to the previous configuration mode or exit 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:`

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:`

help	Shows how to use help
?	Shows options for command completion (context sensitive)

System Management Commands

These commands are used to control system logs, passwords, user names, browser configuration options, and display or configure a variety of other system information.

System Management Commands

Command Group	**Function**	**Page #**
• **Device Designation**	Configures information that uniquely identifies this switch	172
• **User Access**	Configures the basic user names and passwords for management access	172
• **IP Filter**	Configures IP addresses that are allowed management access	173
• **Web Server**	Enables management access via a web browser	175
• **Telnet Server**	Enables management access via Telnet	176
• **Secure Shell**	Provides secure replacement for Telnet	176
• **Event Logging**	Controls logging of error messages	181
• **SMTP Alerts**	Configures SMTP email alerts	185
• **Time Commands**	Sets the system clock automatically via NTP/SNTP server or manually	187
• **System Status**	Displays system configuration, active managers, and version information	189

Device Designation Commands

Device Designation Commands

Command	Function

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 FE-PoE`
	`FE-PoE(config)#`

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)#`

snmp-server contact	Sets the system contact string
snmp-server location	Sets the system location string

User Access Commands

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 165), user authentication via a remote authentication server (page 224), and host access authentication for specific ports (page 205).

User Access Commands

Command	Function

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>
<tr><th colspan="2">Device Designation Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Function</th></tr>
<tr><td><b>username (Cont.)</b></td><td>:<table><tr><th>username</th><th>access-level</th><th>password</th></tr><tr><td>guest</td><td>0</td><td>guest</td></tr></table><b>Command Mode</b>: Global Configuration
<b>Command Usage</b>: 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.
<b>Example</b>: This example shows how to set the access level and password for a user.
<code>Console(config)#username bob access-level 15</code>
<code>Console(config)#username bob password 0 smith</code>
<code>Console(config)#</code></td></tr>
<tr><td><b>enable password</b>
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.</td><td><b>Syntax</b>:
<code>enable password [level level] {0 | 7} password</code>
<code>no enable password [level level]</code>
• 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
<b>Default Setting:</b>
• The default is level 15.
• The default password is “<i>super</i>”
<b>Command Mode:</b> Global Configuration
<b>Command Usage</b>: 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 (page 4-19). 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:
<code>Console(config)#enable password level 15 0 admin</code>
<code>Console(config)#</code></td></tr>
</table>

IP Filter Commands

<table>
<tr><th colspan="2">IP Filter Commands</th></tr>
<tr><th>Command</th><th>Function</th></tr>
<tr><td><b>management</b>
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.</td><td><b>Syntax</b>:
<code>[no] management {all-client | http-client | snmp-client | telnet-client} start-address [end-address]</code>
• all-client - Adds IP address(es) to the SNMP, web and Telnet 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.
<b>Default Setting</b>: All addresses
<b>Command Mode</b>: Global Configuration</td></tr>
</table>

IP Filter Commands (Cont.)

<table>
<tr><th>Command</th><th>Function</th></tr>
<tr><td>

management (Cont.)

</td><td>

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(config)#
```

</td></tr>
<tr><td>

show management

This command displays the client IP addresses that are allowed management access to the switch through various protocols.

</td><td>

Syntax:

```
show management {all-client | http-client | snmp-client | telnet-client}
```

- all-client - Adds IP address(es) to the SNMP, web and Telnet 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.

Command Mode: Global Configuration

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#
```

</td></tr>
</table>

Web Server Commands

Web Server Commands	
Command	**Function**

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)#`

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)#`

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 and Netscape Navigator 4.x or later versions.
	• The following web browsers and operating systems currently support HTTPS
	Internet Explorer 5.0 or later: Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP.
	Netscape Navigator 6.2 or later: Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6
	• To specify a secure-site certificate, see the *Replacing the Default Secure-Site Certificate* section on page 60.
	Example:
	`Console(config)#ip http secure-server`
	`Console(config)#`

Web Server Commands (Cont.)	
Command	**Function**

ip http secure-port
This command specifies the UDP port number used for HTTPS/SSL 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/SSL. (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)#`

Time Commands	
calendar set	Set the system clock
show calendar	Displays the system clock

Telnet Server Commands

Telnet Server Commands	
Command	**Function**

ip telnet port
This command specifies the TCP port number used by the Telnet interface.
Use the no form to use the default port.
	Syntax:
	`ip telnet port port-number`
	`no ip telnet port`
	• port-number - The TCP port to be used by the browser interface. Range: 1-65535
	Default Setting: 23
	Command Mode: Global Configuration
	Example:
	`Console(config)#ip telnet port 123`
	`Console(config)#`

ip telnet server
This command allows this device to be monitored or configured from Telnet.
Use the no form to disable this function.
	Syntax:
	`[no] ip telnet server`
	Default Setting: Enabled
	Command Mode: Global Configuration
	Example:
	`Console(config)#ip telnet server`
	`Console(config)#`

Secure Shell Commands

The Berkley-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 Berkley remote access tools. SSH can also provide remote management access to this switch as a secure replacement for Telnet. When a client contacts the switch via the SSH protocol, the switch uses a public-key that the client must match along with a local user name and password for access authentication.

NOTE

The switch supports SSH version 1.5 and 2.0.

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 (see page 199).
- 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

1. **Generate a Host Key Pair** – Use the **ip ssh crypto host-key generate** command (see page 179) 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 10825913212890233
   76546801726272571413428762941301196195566782 595664104869574278881462065
   194174677298486546861571773939016477935594230357741309802273708779454524083971
   752646358058176716709574804776117
   ```

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 as described on page 172.) 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 134108168560989392104094492015542534763164192187295892114317388005553616163105177594083868631109291232226828519254374603100937187721199696317813662774141689851320491172048303392543241016379975923714490119380060902539484084827178194372288402533115952134861022902978982721353267131629432532818915045306393916643 steve@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 (see page 178) to enable the SSH server on the switch.
6. **Configure Challenge-Response 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 gain access. The following exchanges take place during this process:
   a. The client sends its 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 the public key to encrypt a random sequence of bytes, and sends this string to the client.
   d. The client uses its private key to decrypt the bytes, and sends the decrypted bytes back to the switch.

The switch compares the decrypted bytes to the original bytes it sent. If the two sets match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

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.

This section describes the commands used to configure the SSH server. However, note that you also need to install a SSH client on the management station when using this protocol to configure the switch.

Secure Shell Commands

Command	Function

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 the host key before enabling the SSH server.
	Example:
	`Console#ip ssh crypto host-key generate dsa`
	`Console#configure`
	`Console(config)#ip ssh server`
	`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)#`

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)#`

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)#`

Secure Shell Commands (Cont.)

Command	Function
copy tftp public-key	Copies the user's public key from a TFTP server to the switch

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:
		• 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#`

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#`

ip ssh save host-key
This command saves host key from RAM to flash memory.
	Syntax:
	`ip ssh save host-key [dsa
		rsa]`
		• dsa – DSA key type.
		• rsa – RSA key type.
		Default Setting: Saves both the DSA and RSA key.
		Command Mode: Privileged Exec
		Example:
		`Console#ip ssh save host-key dsa`
		`Console#`

<table>
<tr><th colspan="3">Secure Shell Commands (Cont.)</th></tr>
<tr><th>Command</th><th colspan="2">Function</th></tr>
<tr><td><b>show ip ssh</b>
This command displays the connection settings used when authenticating client access to the SSH server.</td><td colspan="2"><b>Command Mode</b>: Privileged Exec
<b>Example</b>:<pre>
Console#show ip ssh
SSH Enabled - version 1.99
Negotiation timeout: 120 secs; Authentication retries: 3
Server key size: 768 bits
Console#
</pre></td></tr>
<tr><td rowspan="8"><b>show ssh</b>
This command displays the current SSH server connections.</td><td colspan="2"><b>Command Mode</b>: Privileged Exec
<b>Example</b>:<pre>
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#
</pre></td></tr>
<tr><td colspan="2"><b>show ssh - display description</b></td></tr>
<tr><td><b>Field</b></td><td><b>Description</b></td></tr>
<tr><td><i>Session:</i></td><td>The session number. (Range: 0-3)</td></tr>
<tr><td><i>Version:</i></td><td>The Secure Shell version number.</td></tr>
<tr><td><i>State:</i></td><td>The authentication negotiation state.
(Values: Negotiation-Started, Authentication-Started, Session-Started)</td></tr>
<tr><td><i>Username:</i></td><td>The user name of the client.</td></tr>
<tr><td><i>Encryption:</i></td><td>The encryption method is automatically negotiated between the client and server.
Options for SSHv1.5 include: DES, 3DES
Options for SSHv2.0 can include different algorithms for the client-to-server (ctos) and server-to-client (stoc):
• aes128-cbc-hmac-sha1
• aes192-cbc-hmac-sha1
• aes256-cbc-hmac-sha1
• 3des-cbc-hmac-sha1
• blowfish-cbc-hmac-sha1
• aes128-cbc-hmac-md5
• aes192-cbc-hmac-md5
• aes256-cbc-hmac-md5
• 3des-cbc-hmac-md5
• blowfish-cbc-hmac-md5
Terminology:
• DES – Data Encryption Standard (56-bit key)
• 3DES – Triple-DES (Uses three iterations of DES, 112-bit key)
• aes – Advanced Encryption Standard (160 or 224-bit key)
• blowfish – Blowfish (32-448 bit key)
• cbc – cypher-block chaining
• sha1 – Secure Hash Algorithm 1 (160-bit hashes)
• md5 – Message Digest algorithm number 5 (128-bit hashes)</td></tr>
</table>

Secure Shell Commands (Cont.)

Command	Function

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 35`
	`156849954018676692593339467750546173253136748908365472541502024 5593`
	`199868544358361651999923329781766065830958610825913212890233765 4680`
	`172627257141342876294130119619556678259566410486957427888146206 5194`
	`174677298486546861571773939016477935594230357741309802273708779 4545`
	`24083971752646358058176716709574804776117`
	`DSA:`
	`ssh-dss AAAB3NzaC1kc3MAAACBAPWKZTPbsRIB8ydEXcxM3dyV/yrDbKStIlnzD/`
	`Dg0h2Hxc YV44sXZ2JXhamLK6P8bvuiyacWbUW/`
	`a4PAtp1KMSdqsKeh3hKoA3vRRSy1N2XFfAKxl5fwFfv`
	`JlPdOkFgzLGMinvSNYQwiQXbKTBH0Z4mUZpE85PWxDZMaCNBPjBrRAAAAFQChb4vsdf`
	`QGNIjwbvwrNLaQ77isiwAAAIEAsy5YWDC99ebYHNRj5kh47wY4i8cZvH+/`
	`p9cnrfwFTMU01VFDly3IR 2G395NLy5Qd7ZDxfA9mCOfT/`
	`yyEfbobMJZi8oGCstSNOxrZZVnMqWrTYfdrKX7YKBw/Kjw6Bm`
	`iFq7O+jAhf1Dg45loAc27s6TLdtny1wRq/`
	`ow2eTCD5nekAAACBAJ8rMccXTxHLFAczWS7EjOy`
	`DbsloBfPuSAb4oAsyjKXKVYNLQkTLZfcFRu41bS2KV5LAwecsigF/`
	`+DjKGWtPNIQqabKgYCw2 o/`
	`dVzX4Gg+yqdTlYmGA7fHGm8ARGeiG4ssFKy4Z6DmYPXFum1Yg0fhLwuHpOSKdxT3kk4`
	`75S7 w0W`
	`Console#`

show users	Shows SSH users, including privilege level and public key type

Event Logging Commands

Event Logging Commands

Command	Function

logging on
This command controls logging of error messages, sending debug or error messages to switch memory.
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. You can use the logging history command to control the type of error messages that are stored.
	Example:
	`Console(config)#logging on`
	`Console(config)#`

<table>
<tr><th colspan="4">Event Logging Commands (Cont.)</th></tr>
<tr><th>Command</th><th colspan="3">Function</th></tr>
<tr><td rowspan="12"><b>logging history</b>
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.</td><td colspan="3"><b>Syntax</b>:
<code>logging history {flash | ram} level</code>
<code>no logging history {flash | ram}</code>
• 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).</td></tr>
<tr><td colspan="3"><b>Logging Levels</b></td></tr>
<tr><td><b>Level</b></td><td><b>Severity Name</b></td><td><b>Description</b></td></tr>
<tr><td>7</td><td>debugging</td><td>Debugging messages</td></tr>
<tr><td>6</td><td>informational</td><td>Informational messages only</td></tr>
<tr><td>5</td><td>notifications</td><td>Normal but significant condition, such as cold start</td></tr>
<tr><td>4</td><td>warnings</td><td>Warning conditions (e.g., return false, unexpected return)</td></tr>
<tr><td>3</td><td>errors</td><td>Error conditions (e.g., invalid input, default used)</td></tr>
<tr><td>2</td><td>critical</td><td>Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)</td></tr>
<tr><td>1</td><td>alerts</td><td>Immediate action needed</td></tr>
<tr><td>0</td><td>emergencies</td><td>System unusable</td></tr>
<tr><td colspan="3"><b>Default Setting</b>:
• Flash: errors (level 3 - 0)
• RAM: warnings (level 7 - 0)
<b>Command Mode</b>: Global Configuration
<b>Command Usage</b>: The message level specified for flash memory must be a higher priority (i.e., numerically lower) than that specified for RAM.
<b>Example</b>:
<code>Console(config)#logging history ram 0</code>
<code>Console(config)#</code></td></tr>
<tr><td><b>logging host</b>
This command adds a syslog server host IP address that will receive logging messages.
Use the no form to remove a syslog server host.</td><td colspan="3"><b>Syntax</b>
<code>[no] logging host host_ip_address</code>
• host_ip_address - The IP address of a syslog server.
<b>Default Setting</b>: None
<b>Command Mode</b>: Global Configuration
<b>Command Usage</b>:
• By using this command more than once you can build up a list of host IP addresses.
• The maximum number of host IP addresses allowed is five.
<b>Example</b>:
<code>Console(config)#logging host 10.1.0.3</code>
<code>Console(config)#</code></td></tr>
</table>

Event Logging Commands (Cont.)

Command	Function

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
	`[no] logging facility type`
	• 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 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]`
	`no logging trap`
	• level - One of the level arguments listed below. Messages sent include the selected level up through level 0.
	Default Setting:
	• Enabled
	• Level 7 - 0
	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 logging
This command clears messages from the log buffer.
	Syntax
	`clear logging [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 logging`
	`Console#`

Event Logging Commands (Cont.)

Command	Function
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.	See below

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.
- 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), 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#
```

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#
```

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.

Event Logging Commands (Cont.)	
Command	**Function**

show log
This command displays the system and event messages stored in memory.
	Syntax:
	• show log {flash | ram} [login] [tail]
	• 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).
	• tail - Shows event history starting from the most recent entry.
	• login - Shows the login record only.
	Default Setting: None
	Command Mode: Privileged Exec
	Command Usage: This command shows the system and event messages stored in memory, including the time stamp, message level, program module, function, and event number.
	Example: The following example shows sample messages stored in RAM:
	`Console#show log ram`
	`[5] 00:01:06 2001-01-01`
	`   "STA root change notification."`
	`   level: 6, module: 6, function: 1, and event no.: 1`
	`[4] 00:01:00 2001-01-01`
	`   "STA root change notification."`
	`   level: 6, module: 6, function: 1, and event no.: 1`
	`[3] 00:00:54 2001-01-01`
	`   "STA root change notification."`
	`   level: 6, module: 6, function: 1, and event no.: 1`
	`[2] 00:00:50 2001-01-01`
	`   "STA topology change notification."`
	`   level: 6, module: 6, function: 1, and event no.: 1`
	`[1] 00:00:48 2001-01-01`
	`   "VLAN 1 link-up notification."`
	`   level: 6, module: 6, function: 1, and event no.: 1`
	`Console#`

SMTP Alert Commands

Configures SMTP event handling, and forwarding of alert messages to the specified SMTP servers and email recipients.

SMTP Alert Commands	
Command	**Function**

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 192.168.1.200`
	`Console(config)#`

SMTP Alert Commands (Cont.)

Command	Function

logging sendmail level
This command sets the severity threshold used to trigger alert messages.
	Syntax:
	`logging sendmail level level`
	• level - One of the system message levels. 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 4 through 0:
	`Console(config)#logging sendmail level 4`
	`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 delete the source email address.
	Syntax:
	`[no] logging sendmail source-email email-address`
	• email-address - The source email address used in alert messages. Range: 0-41 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: This example will set the source email john@acme.com:
	`Console(config)#logging sendmail source-email john@acme.com`
	`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
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)#`

SMTP Alert Commands (Cont.)

Command	Function

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`
	`-----------------------------------------------`
	`  1. 192.168.1.200`
	
	`SMTP minimum severity level: 4`
	
	`SMTP destination email addresses`
	`-----------------------------------------------`
	`  1. geoff@acme.com`
	
	`SMTP source email address:   john@acme.com`
	
	`SMTP status:                Enabled`
	`Console#`

Time Commands

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.

Time Commands

Command	Function

sntp client
This command enables SNTP client requests for time synchronization from NTP or SNTP time servers specified with the sntp servers 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 servers 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: 10.1.0.19 0.0.0.0 0.0.0.0`
	`Current server: 10.1.0.19`
	`Console#`

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.
	Syntax:
	`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`

Time Commands (Cont.)

Command	**Function**

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(config)#`

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:  Dec 23 05:13:28 2002`
	`Poll interval: 16`
	`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#`

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: 1-29 characters)
	• hours - Number of hours before/after UTC. (Range: 1-12 hours)
	• 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)#`

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
	Example: This example shows how to set the system clock to 15:12:34, April 1st, 2004:
	`Console#calendar set 15 12 34 1 April 2004`
	`Console#`

Time Commands (Cont.)

Command	Function

show calendar
This command displays the system clock.
	Default Setting: None
	Command Mode: Normal Exec, Privileged Exec
	Example:
	`Console#show calendar`
	` 15:12:34 April 1 2004`
	`Console#`

System Status Commands

System Status Commands

Command	Function

light unit
This command displays the unit ID of a switch using its front-panel LED indicators.
	Syntax:
	`light unit [unit]`
	• unit - specifies a unit in a switch stack to light the panel LEDs
	Default Setting: None
	Command Mode: Normal Exec, Privileged Exec
	Command Usage: The unit ID is displayed using the port status LED indicators for ports 1 to 8. When the light unit command is entered, the LED corresponding to the switch's ID will flash for about 15 seconds.
	Example:
	`Console#light unit 1`
	`Console#`

show startup-config
This command displays the configuration file stored in non-volatile memory that is used to start up the system.
	Default Setting: None
	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:
	• SNMP community strings
	• Users (names and access levels)
	• VLAN database (VLAN ID, name and state)
	• VLAN configuration settings for each interface
	• IP address configured for the switch
	• Spanning tree settings
	• Any configured settings for the console port and Telnet
	Example:
	`Console#show startup-config`
	`building startup-config, please wait.....`
	`!`
	`!`
	`username admin access-level 15`
	`username admin password 0 admin`
	`!`
	`username guest access-level 0`
	`username guest password 0 guest`
	`!`
	`enable password level 15 0 super`
	`!`
	`snmp-server community public ro`
	`snmp-server community private rw`
	`!`
	`logging history ram 6`
	`logging history flash 3`
	`!`

System Status Commands (Cont.)

Command	Function

show startup-config (Cont.)	`vlan database`
	` vlan 1 name DefaultVlan media ethernet state active`
	`!`
	`interface ethernet 1/1`
	` switchport allowed vlan add 1 untagged`
	` switchport native vlan 1`
	`.`
	`.`
	`.`
	`interface vlan 1`
	` ip address dhcp`
	`!`
	`line console`
	`!`
	`line vty`
	`!`
	`end`
	
	`Console#`

show running-config
This command displays the configuration information currently in use.
	Default Setting: None
	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 each switch in the stack
	• SNTP server settings
	• SNMP community strings
	• Users (names, access levels, and encrypted passwords)
	• Event log settings
	• VLAN database (VLAN ID, name and state)
	• VLAN configuration settings for each interface
	• IP address configured for the switch
	• Layer 4 precedence settings
	• Any configured settings for the console port and Telnet
	Example:
	`Console#show running-config`
	`building running-config, please wait.....`
	`!`
	`phymap 5a-a5-aa-55-44-32 00-00-00-00-00-00 00-00-00-00-00-00 00-00-00-`
	`00-00-00 00-00-00-00-00-00 00-00-00-00-00-00 00-00-00-00-00-00 00-00-`
	`00-00-00-00`
	`!`
	`SNTP server 0.0.0.0 0.0.0.0 0.0.0.0`
	`!`
	`!`
	`!`
	`SNMP-server community private rw`
	`SNMP-server community public ro`
	`!`
	`!`
	`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`
	`!`
	`!`
	`logging history ram 6`
	`logging history flash 3`
	`!`

<table>
<tr><th colspan="2">System Status Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Function</th></tr>
<tr><td><b>show running-config (Cont.)</b></td><td><pre>
vlan database
 vlan 1 name DefaultVlan media ethernet state active
!
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
.
.
.
!
interface vlan 1
 ip address DHCP
!
!
no map IP precedence
no map IP DSCP
!
!
line console
!
line vty
!
end
!
Console#
</pre></td></tr>
<tr><td><b>show system</b>
This command displays system information.</td><td><b>Default Setting</b>: None
<b>Command Mode</b>: Normal Exec, Privileged Exec
<b>Command Usage</b>: For a description of the items shown by this command, refer to “Displaying System Information” on page 3-9.
The POST results should all display “PASS.” If any POST test indicates “FAIL,” contact your distributor for assistance.
<b>Example</b>:<pre>
Console#show system
System description: 24FE Stackable Intelligent Switch
System OID string: 1.3.6.1.4.1.259.6.10.61
System information
 System Up time: 0 days, 0 hours, 0 minutes, and 7.18 seconds
 System Name: [NONE]
 System Location: [NONE]
 System Contact: [NONE]
 MAC address: 5A-A5-AA-55-44-32
 Web server: enabled
 Web server port: 80
 Web secure server: enabled
 Web secure server port: 443
 Telnet server: enable
 Telnet port: 23
 Jumbo Fram: Disabled
 POST result
POST result
UART LOOP BACK Test..........PASS
DRAM Test....................PASS
Timer Test...................PASS
PCI Device 1 Test............PASS
PCI Device 2 Test............PASS
Switch Int Loopback test.....PASS

Done All Pass.
Console#
</pre></td></tr>
</table>

<table>
<tr><th colspan="2">System Status Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Function</th></tr>
<tr><td>

show users

Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet client.

</td><td>

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
 Username accounts:
  Username 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 Username Idle time (h:m:s).
  ----------- -------------- -------- ------------------
 1      HTTP   192.168.1.19    admin           0:00:00

Console#
```

</td></tr>
<tr><td>

show version

This command Displays hardware and software version information for the system.

</td><td>

Default Setting: None

Command Mode: Normal Exec, Privileged Exec

Command Usage: See “Displaying Switch Hardware/Software Versions” on page 3-10 for detailed information on the items displayed by this command.

Example:

```
Console#show version
Unit1
 Serial number           :A322043872
 Hardware version        :R0A
 Module A type           :Combo 1000BaseT SFP
 Module B type           :Combo 1000BaseT SFP
Number of ports          :26
 Main power status       :up
 Redundant power status :not present

Agent(master)
 Loader version:          2.2.1.1
 Boot ROM version:        2.2.1.2
 Operation code version:  2.2.5.3
Console#
```

</td></tr>
</table>

Flash/File Commands

These commands are used to manage the system code or configuration files.

Flash/File Commands

Command	**Function**

copy
This command moves (upload/ download) a code image or configuration file between the switch's flash memory and a TFTP server.
When you save the system code or configuration settings to a file on a 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 | running-config | startup-config | tftp | unit}`
	`copy running-config {file | startup-config | tftp}`
	`copy startup-config {file | running-config | tftp}`
	`copy tftp {file | running-config | startup-config | https-certificate | public-key}`
	`copy unit file`
	• file - Keyword that allows you to copy to/from a file.
	• 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.
	• https-certificate - Copies an HTTPS certificate from an TFTP server to the switch.
	• public-key - Keyword that allows you to copy a SSH key from a TFTP server. ("Secure Shell Commands" on page 4-34)
	• unit - Keyword that allows you to copy to/from a unit.
	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 /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")
	• Due to the size limit of the flash memory, the switch supports only two operation code files.
	• The maximum number of user-defined configuration files depends on available memory.
	• 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.
	• Use the copy file unit command to copy a local file to another switch in the stack. Use the copy unit file command to copy a file from another switch in the stack.
	• The Boot ROM and Loader cannot be uploaded or downloaded from the TFTP server. You must follow the instructions in the release notes for new firmware, or contact your distributor for help.
	• For information on specifying an https-certificate, see "Replacing the Default Secure-site Certificate" on page 3-42. For information on configuring the switch to use HTTPS/SSL for a secure connection, see "ip http secure-server" on page 4-31.
	Example: 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#`

Flash/File Commands (Cont.)	
Command	**Function**

copy
(Cont.)
	Example:
	The following example shows how to copy the running configuration to a startup file:
	`Console#copy running-config file`
	`destination file name: startup`
	`Write to FLASH Programming.`
	`\Write to FLASH finish.`
	`Success.`
	
	`Console#`
	Example:
	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#`
	Example:
	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`
	Example:
	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: <1-2>: 1`
	`Source file name: steve.pub`
	`Username: steve`
	`TFTP Download`
	`Success.`
	`Write to FLASH Programming.`
	`Success.`
	
	`Console#`

delete
This command deletes a file or image.
	Syntax:
	`delete [unit:] filename`
	• filename - Name of the configuration file or image name.
	• unit - Stack unit. (Range: 1-8)
	Default Setting: None
	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.
	• A colon (:) is required after the specified unit number.
	Example: This example shows how to delete the test2.cfg configuration file from flash memory for unit 1:
	`Console#delete 1:test2.cfg`
	`Console#`

Flash/File Commands (Cont.)

Command

Function

dir

This command displays a list of files in flash memory.

Syntax:

```
dir [unit:] {{boot-rom: | config: | opcode:} [:filename]}
```

The type of file or image to display includes:

- boot-rom - Boot ROM (or diagnostic) image file.
- config - Switch configuration file.
- opcode - Run-time operation code image file.
- filename - Name of the configuration file or image name.
- unit - Stack unit. (Range: 1-8)

Default Setting: None

Command Mode: Privileged Exec

Command Usage: If you enter the command dir without any parameters, the system displays all files.

- A colon (:) is required after the specified unit number.

File information is shown below:

- 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 1:
          file name                     file type       startup size (byte)
 -----------------------------------     --------------  ------- ---------
--
 Unit1:
          DIAG_0.0.0.4.BIX              Boot-Rom image  Y           169900
          LEO_50Y_V0.0.5.1.bix          Operation Code  Y          1614764
          Factory_Default_Config.cfg    Config File     N             5013
         startup                        Config File     Y             3191
 -------------------------------------------------------------------------
                                                Total free space:   5242880
Console#
```

whichboot

This command displays which files were booted when the system powered up.

Syntax:

```
whichboot [unit]
```

- unit - Specifies the unit number.

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:
        diag_0060 Boot-Rom image       Y      111360
         run_0200 Operation Code       Y     1083008
          startup    Config File       Y        2710
Console#
```

Flash/File Commands (Cont.)	
Command	**Function**

boot system
This command specifies the image used to start up the system.
	Syntax:
	`boot system [unit:] {boot-rom| config | opcode}: filename`
	The type of file or image to set as a default includes:
	• boot-rom - Boot ROM (required).
	• config - Configuration file (required).
	• opcode - Run-time operation code (required).
	• filename - Name of the configuration file or image name.
	• unit - Specifies the unit number (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.
	A colon (:) is required after the specified unit number.
	Example:
	`Console(config)#boot system config: startup`
	`Console(config)#`

Power over Ethernet (PoE) Commands

The commands in this group control the power that can be delivered to attached PoE devices through the switch ports.

The switch’s power management enables total switch power and individual port power to be controlled within a configured power budget. Port power can be automatically turned on and off for connected devices, and a per-port power priority can be set so that the switch never exceeds its allocated power budget.

When a device is connected to a switch port, its power requirements are detected by the switch before power is supplied. If the power required by a device exceeds the power budget of the port or the whole switch, power is not supplied.

PoE Commands	
Command	**Function**

power mainpower maximum allocation
Use this command to define a power budget for the switch (power available to all switch ports).
Use the no form to restore the default setting.
	Syntax:
	`power mainpower maximum allocation <watts> [unit unit]`
	• unit - The switch unit in the stack.
	• watts - The power budget for the switch. (Range: 36 - 800 watts)
	Default Setting: 375 watts
	Command Mode: Privileged Executive
	Command Usage: Setting a maximum power budget for the switch enables power to be centrally managed, preventing overload conditions at the power source.
	If the power demand from devices connected to the switch exceeds the power budget setting, the switch uses port power priority settings to limit the supplied power.
	Example:
	`Console(config)#power mainpower maximum allocation 300`
	`Console(config)#`

PoE Commands (Cont.)

Command	Function

power inline
Use this command to turn power on for a specific port or force a port into test mode.
Use the no form to turn off power for a port.
	Syntax:
	`power inline [auto | test]`
	`no power inline`
	• auto - The switch automatically detects if a device is connected to the port and turns power on or off accordingly.
	• test - Forces the port into a test mode. In test mode the port continuously attempts to detect if a device is connected to the port, but does not supply power.
	Default Setting: auto
	Command Mode: Interface Configuration
	Command Usage: Using the command without an argument enables port power in auto mode (the same as the power inline auto command).
	In the default auto mode, power is automatically supplied when a device is detected on the port, providing that the power demanded does not exceed switch's power budget.
	Example:
	`Console(config)#interface ethernet 1/1`
	`Console(config-if)#power inline auto`
	`Console(config-if)#exit`
	`Console(config)#interface ethernet 1/2`
	`Console(config-if)#no power inline`
	`Console(config-if)#`

power inline maximum allocation
Use this command to limit the power allocated to specific ports.
Use the no form to restore the default setting.
	Syntax:
	`power inline maximum allocation [milliwatts]`
	`no power inline maximum allocation`
	• milliwatts - The maximum power budget for the port. Range: 3000 - 15400 milliwatts.
	Default Setting: 15400 milliwatts
	Command Mode: Interface Configuration
	Command Usage: If a device is connected to a switch port and the switch detects that it requires more than the maximum power allocated to the port, no power is supplied to the device (the port power remains off).
	Example:
	`Console(config)#interface ethernet 1/1`
	`Console(config-if)#power inline maximum allocation 8000`
	`Console(config-if)#`

power inline priority
Use this command to set the power priority for specific ports.
Use the no form to restore the default setting.
	Syntax:
	`power inline priority priority`
	`no power inline priority`
	• priority - The power priority for the port.
	Options: 1 (critical), 2 (high), or 3 (low).
	Default Setting: 3 (low)
	Command Mode: Interface Configuration
	Command Usage: If the power demand from devices connected to the switch exceeds the power budget setting, the switch uses port power priority settings to control the supplied power. For example:
	• A device connected to a low-priority port that causes the switch to exceed its budget is not supplied power.
	• A device connected to a critical or high-priority port that causes the switch to exceed its budget is supplied power, but the switch drops power to one or more lower-priority ports.
	• Power is dropped from low-priority ports in sequence starting from port number 1.
	Example:
	`Console(config)#interface ethernet 1/1`
	`Console(config-if)#power inline priority 2`
	`Console(config-if)#`

<table>
<tr><th colspan="2">PoE Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Function</th></tr>
<tr><td>

show power inline status

Use this command to display the current power status for all ports or for specific ports.

</td><td>

Syntax:

<pre>
show power inline status [interface]
interface
ethernet
</pre>

- unit - This is device 1.
- port - Physical port number on the switch (Range: 1-26).

Command Mode: Privileged Exec

Command Usage: This command displays the following parameters:

- Admin: The power mode set on the port (see the *power inline* section on page 197)
- Oper: The current operating power status (displays on or off)
- Power (mWatt): Displays a list of files in flash memory
- Power (used): The current power consumption on the port in milliwatts
- Priority: The port’s power priority setting (see the *power inline priority* on page 197)

Example:

<pre>
Console#show power inline status
Interface Admin   Oper Power(mWatt) Power(used) Priority
---------- ------- ---- ------------ ------------ --------
Eth   1/ 1 enable off   15400   0   low
Eth   1/ 2 enable off   15400   0   low
Eth   1/ 3 enable   on   15400   7505   low
Eth   1/ 4 enable off   15400   0   low
Eth   1/ 5 enable off   15400   0   low
Eth   1/ 6 enable off   15400   0   low
Eth   1/ 7 enable   on   15400   8597   low
.
.
.
Eth   1/23 enable off   15400   0   low
Eth   1/24 enable off   15400   0   low
Console#
</pre>

</td></tr>
<tr><td>

show power mainpower

Use this command to display the current power status for the switch.

</td><td>

Command Mode: Privileged Exec

Command Usage: This command displays the following parameters:

- Maximum Available Power: The available power budget for the switch (see the *power mainpower maximum allocation* on page 196)
- System Operation Status: The current operating power status (displays on or off)
- Mainpower Consumption: The current power consumption on the switch in watts
- Software Version: The version of software running on the PoE controller subsystem in the switch. This software can be updated using the **copy file controller** command (page 193 see page 55).

Example:

<pre>
Console#show power mainpower
Unit 1 Mainpower Status
 Maximum Available Power : 375 watts
 System Operation Status : on
 Mainpower Consumption   : 15 watts
 Software Version   : Version 0x1B64, Build 0x07
Console#
</pre>

</td></tr>
</table>

Authentication Commands

You can configure this switch to authenticate users logging into the system for management access using local or RADIUS authentication methods. You can also enable port-based authentication for network client access using IEEE 802.1x.

Authentication Commands	
Command	**Function**

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)#`

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 (see page 169).
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)#`

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.

RADIUS Client Commands

Command	**Function**

radius-server host
This command specifies primary and backup RADIUS servers and authentication parameters that apply to each server.
Use the no form to restore the default values.
	Syntax:
	`[no] radius-server index host {host_ip_address | host_alias}`
	`[auth-port auth_port] [timeout timeout] [retransmit retransmit]`
	`[key key]`
	• 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.
	• host_alias - Symbolic name of server. (Maximum length: 20 characters)
	• port_number - RADIUS server UDP port used for authentication messages. (Range: 1-65535)
	• timeout - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)
	• retransmit - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1-30)
	• key - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)
	Default Settings:
	• auth-port - 1812
	• timeout - 5 seconds
	• retransmit - 2
	Command Mode: Global Configuration
	Example:
	`Console(config)#radius-server 1 host 192.168.1.20 auth-port 181`
	`timeout 10 retransmit 5 key green`
	`Console(config)#`

radius-server port
This command sets the RADIUS server network port.
Use the no form to restore the default.
	Syntax:
	`radius-server port port_number`
	`no radius-server 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 port 181`
	`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: 20 characters)
	Default Setting: None
	Command Mode: Global Configuration
	Example:
	`Console(config)#radius-server key green`
	`Console(config)#`

RADIUS Client Commands (Cont.)

Command	**Function**

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`
	` Communication key with RADIUS server:`
	` Server port number:                   1812`
	` Retransmit times:                     2`
	` Request timeout:                      5`
	
	`Sever 1:`
	` Server IP address: 192.168.1.1`
	` Communication key with RADIUS server:`
	` Server port number:                   1812`
	` Retransmit times:                     2`
	` Request timeout:                      5`
	
	`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.

TACACS+ Client Commands

Command	**Function**

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 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 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: 20 characters)
	Default Setting: None
	Command Mode: Global Configuration
	Example:
	`Console(config)#tacacs-server key green`
	`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:`
	` Server IP address:                     10.11.12.13`
	` Communication key with TACACS server: *****`
	` Server port number:                    49`
	`Console#`

Port Security Commands

These commands can be used to disable the learning function or manually specify secure addresses for a port. You may want to leave port security off for an initial training period (i.e., enable the learning function) to register all the current VLAN members on the selected port, and then enable port security to ensure that the port will drop any incoming frames with a source MAC address that is unknown or has been previously learned from another port.

Port Security Commands

Command	Function

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)
	Default Settings:
	• Status: Disabled
	• Action: None
	• Maximum Addresses: 0
	Command Mode: Interface Configuration (Ethernet)
	Command Usage: If you enable 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 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.
	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 use port monitoring.
	• Cannot be a multi-VLAN port.
	• 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`

Port Security Commands (Cont.)

Command	Function

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 - Stack unit. (Range: 1-8)
	port - Port number. (Range: 1-26)
	port-channel *channel-id* (Range: 1-4)
	• 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`

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 - Stack unit. (Range: 1-8) port - Port number. (Range: 1-26) port-channel *channel-id* (Range: 1-4) • 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.

Port Security Commands (Cont.)

Command	Function

show mac-address-table (Cont.)	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-de    1  Delete-on-reset`
	`  Trunk 2 00-E0-29-8F-AA-1B    1  Learned`
	`Console#`

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).

802.1x Port Authentication Commands

Command	Function

dot1x system-auth-control
This command enables 802.1X port authentication globally on the switch.
Use the no form to restore the default.
	Syntax:
	`[no] system-auth-control`
	Default Setting: Disabled
	Command Mode: Global Configuration
	Example:
	`Console(config)#dot1x system-auth-control`
	`Console(config)#`

dot1x default
This command sets all configurable dot1x global and port settings to their default values.
	Syntax:
	`dot1x default`
	Command Mode: Global Configuration
	Example:
	`Console(config)#dot1x default`
	`Console(config)#`

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)#`

802.1x Port Authentication Commands (Cont.)

Command	Function

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 operation-mode
This command allows single or multiple 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]}`
	`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: 1-20; Default: 5)
	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 (page 4-83).
	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.
	Example:
	`Console(config)#interface eth 1/2`
	`Console(config-if)#dot1x operation-mode multi-host max-count 10`
	`Console(config-if)#`

dot1x re-authenticate
This command forces re-authentication on all ports or a specific interface.
	Syntax:
	`dot1x re-authenticate [interface]`
	• interface
	ethernet unit/port
	unit - Stack unit. (Range: 1-8)
	port - Port number. (Range: 1-26)
	Command Mode: Privileged Exec
	Example:
	`Console#dot1x re-authenticate`
	`Console#`

dot1x re-authentication
This command enables periodic re-authentication globally for all ports.
Use the no form to disable re-authentication.
	Syntax:
	`[no] dot1x re-authentication`
	Command Mode: Interface Configuration
	Example:
	`Console(config)#interface eth 1/2`
	`Console(config-if)#dot1x re-authentication`
	`Console(config-if)#`

802.1x Port Authentication Commands (Cont.)

Command	Function

dot1x timeout quiet-period
This command sets the time that a switch port waits after the Max Request Count 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.
	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 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)#`

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 - Stack unit. (Range: 1-8) port - Port number. (Range: 1-26) **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. • 802.1X Port Summary – Displays the port access control parameters for each interface, including the following items: *Status*– Administrative state for port access control. Operation Mode– Dot1x port control operation mode (page 4-83). *Mode*– Dot1x port control mode (page 4-83). *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: *reauth-enabled*– Periodic re-authentication (page 4-84). *reauth-period*– Time after which a connected client must be re-authenticated (page 4-85). *quiet-period*– Time a port waits after Max Request Count is exceeded before attempting to acquire a new client (page 4-85).

802.1x Port Authentication Commands (Cont.)	
Command	**Function**
show dot1x (Cont.)	*tx-period*– Time a port waits during authentication session before re-transmitting EAP packet (page 4-86). *supplicant-timeout*– Supplicant timeout. *server-timeout*– Server timeout. *reauth-max*– Maximum number of reauthentication attempts. *max-req*– Maximum number of times a port will retransmit an EAP request/identity packet to the client before it times out the authentication session (page 4-82). *Status*– Authorization status (authorized or not). *Operation Mode*– Shows if single or multiple hosts (clients) can connect to an 802.1X-authorized port. *Max Count*– The maximum number of hosts allowed to access this port (page 4-83). *Port-control*–Shows the dot1x mode on a port as auto, force-authorized, or force-unauthorized (page 4-83). *Supplicant*– MAC address of authorized client. *Current Identifier*– The integer (0-255) used by the Authenticator to identify the current authentication session. • 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. • 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: enable

802.1X Port Summary

Port Name  Status    Operation Mode   Mode
Authorized
1/1       disabled   Single-Host      ForceAuthorized     n/a
1/2       enabled    Single-Host      auto                yes
.
.
.
1/26      disabled   Single-Host      ForceAuthorized     n/a

802.1X Port Details

802.1X is disabled on port 1/1

802.1X is enabled on port 1/2
reauth-enabled:     Enable
 reauth-period:     1800
 quiet-period:      30
 tx-period:         40
 supplicant-timeout:30
 server-timeout:    10
 reauth-max:        2
 max-req:           5
 Status             Authorized
```

<table>
<tr><th colspan="2">802.1x Port Authentication Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Function</th></tr>
<tr><td><b>show dot1x (Cont.)</b></td><td><pre>
Operation mode   Single-Host
Max count   5
Port-control   Auto
Supplicant   00-00-e8-49-5e-dc
Current Identifier 3

Authenticator State Machine
State   Authenticated
Reauth Count   0

Backend State Machine
State   Idle
Request Count   0
Identifier(Server) 2

Reauthentication State Machine
State   Initialize
.
.
.
802.1X is disabled on port 1/26
Console#
</pre></td></tr>
</table>

Access Control List Commands

Access Control Lists (ACL) provide packet filtering for IP frames (based on address, protocol, Layer 4 protocol port number or TCP control code) or any frames (based on MAC address or Ethernet type). To filter packets, first create an access list, add the required rules, specify a mask to modify the precedence in which the rules are checked, and then bind the list to a specific port.

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 or egress 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 for a list of all permit rules, the packet is dropped; and if no rules match for a list of all deny rules, the packet is accepted.

There are three filtering modes:

- Standard IP ACL mode (STD-ACL) filters packets based on the source IP address.
- Extended IP ACL mode (EXT-ACL) filters packets based on source or destination IP address, as well as protocol type and protocol port number.
  If the TCP protocol is specified, then you can also filter packets based on the TCP control code.
- MAC ACL mode (MAC-ACL) filters packets based on the source or destination MAC address and the Ethernet frame type (RFC 1060).

The following restrictions apply to ACLs:

- This switch supports ACLs for both ingress and egress filtering.
  However, you can only bind one IP ACL and one MAC ACL to any port for ingress filtering, and one IP ACL and one MAC ACL to any port for egress filtering. In other words, only four ACLs can be bound to an interface – Ingress IP ACL, Egress IP ACL, Ingress MAC ACL and Egress MAC ACL.
- When an ACL is bound to an interface as an egress filter, all entries in the ACL must be deny rules. Otherwise, the bind operation will fail.
- Each ACL can have up to 32 rules.
- The maximum number of ACLs is also 32. However, due to resource restrictions, the average number of rules bound the ports should not exceed 20.
- You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.
- The switch does not support the explicit “deny any any” rule for the egress IP ACL or the egress MAC ACLs. If these rules are included in ACL, and you attempt to bind the ACL to an interface for egress checking, the bind operation will fail.

- Egress MAC ACLs only work for destination-mac-known packets, not for multicast, broadcast, or destination-mac-unknown packets.

The order in which active ACLs are checked is as follows:

1. User-defined rules in the Egress MAC ACL for egress ports.
2. User-defined rules in the Egress IP ACL for egress ports.
3. User-defined rules in the Ingress MAC ACL for ingress ports.
4. User-defined rules in the Ingress IP ACL for ingress ports.
5. Explicit default rule (permit any any) in the ingress IP ACL for ingress ports.
6. Explicit default rule (permit any any) in the ingress MAC ACL for ingress ports.
7. If no explicit rule is matched, the implicit default is permit all.

Masks for Access Control Lists

You can specify optional masks that control the order in which ACL rules are checked. The switch includes two system default masks that pass/filter packets matching the permit/deny the rules specified in an ingress ACL. You can also configure up to seven user-defined masks for an ACL.

A mask must be bound exclusively to one of the basic ACL types (i.e., Ingress IP ACL, Egress IP ACL, Ingress MAC ACL or Egress MAC ACL), but a mask can be bound to up to four ACLs of the same type.

IP ACL Commandss

IP ACL Commands	
Command	**Function**

access-list ip
This command adds an IP access list and enters configuration mode for standard or extended IP 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)
	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.
	***Note**: An ACL can contain up to 32 rules.*
	Example:
	`Console(config)#access-list ip standard david`
	`Console(config-std-acl)#`

IP ACL Commands (Cont.)

Command	Function

permit, deny
(Standard ACL)
This command adds a rule to a Standard IP ACL. The rule sets a filter condition for packets emanating from the specified source.
Use the no form to remove a rule.
	Syntax:
	`[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.
	Default Setting: None
	Command Mode: Standard ACL
	Command Usage: New rules are appended to the end of the list.
	Address bitmasks 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)#`

permit, deny
(Extended ACL)
This command adds a rule to an Extended IP 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:
	`[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 [end]] [destination-port dport [end]]`
	`[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 [end]] [destination-port dport [end]]`
	`[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 (TCP, UDP or other protocol types) source port number. (Range: 0-65535)
	• dport – Protocol ((TCP, UDP or other protocol types)) destination port number. (Range: 0-65535)
	• end – Upper bound of the protocol port range. (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. (Range: 0-63)
	Default Setting: None
	Command Mode: Extended ACL

IP ACL Commands (Cont.)

Command	Function

permit, deny
(Extended ACL - Cont.)
	Command Usage: All new rules are appended to the end of the list.
	Address bitmasks 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)#`
	Example:
	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)#`
	Example:
	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)#`

IP ACL Commands (Cont.)	
Command	**Function**

show ip access-list
This command displays the rules for configured IP 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 168.92.0.0 255.255.255.0`
	`Console#`

access-list ip mask-precedence
This command changes to the IP Mask mode used to configure access control masks.
Use the no form to delete the mask table.
	Syntax:
	`[no] access-list ip mask-precedence {in | out}`
	• in – Ingress mask for ingress ACLs.
	• out – Egress mask for egress ACLs.
	Default Setting: Default system mask: Filter inbound packets according to specified IP ACLs.
	Command Mode: Global Configuration
	Command Usage: A mask can only be used by all ingress ACLs or all egress ACLs.
	The precedence of the ACL rules applied to a packet is not determined by order of the rules, but instead by the order of the masks; i.e., the first mask that matches a rule will determine the rule that is applied to a packet.
	You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.
	Example:
	`Console(config)#access-list ip mask-precedence in`
	`Console(config-ip-mask-acl)#`

mask
(IP ACL)
This command defines a mask for IP ACLs.
This mask defines the fields to check in the IP header.
Use the no form to remove a mask.
	Syntax:
	`[no] mask [protocol]`
	`{any | host | source-bitmask}`
	`{any | host | destination-bitmask}`
	`[precedence] [tos] [dscp]`
	`[source-port [port-bitmask]] [destination-port [port-bitmask]]`
	`[control-flag [flag-bitmask]]`
	• protocol – Check the protocol field.
	• any – Any address will be matched.
	• host – The address must be for a host device, not a subnetwork.
	• source-bitmask – Source address of rule must match this bitmask.
	• destination-bitmask – Destination address of rule must match this bitmask.
	• precedence – Check the IP precedence field.
	• tos – Check the TOS field.
	• dscp – Check the DSCP field.
	• source-port – Check the protocol source port field.
	• destination-port – Check the protocol destination port field.
	• port-bitmask – Protocol port of rule must match this bitmask. (Range: 0-65535)
	• control-flag – Check the field for control flags.
	• flag-bitmask – Control flags of rule must match this bitmask. (Range: 0-63)
	Default Setting: None
	Command Mode: IP Mask

IP ACL Commands (Cont.)	
Command	**Function**

mask
(IP ACL - Cont.)
	Command Usage: Packets crossing a port are checked against all the rules in the ACL until a match is found. The order in which these packets are checked is determined by the mask, and not the order in which the ACL rules were entered.
	First create the required ACLs and ingress or egress masks before mapping an ACL to an interface.
	If you enter dscp, you cannot enter tos or precedence. You can enter both tos and precedence without dscp.
	Masks that include an entry for a Layer 4 protocol source port or destination port can only be applied to packets with a header length of exactly five bytes.
	Example: This example creates an IP ingress mask with two rules. Each rule is checked in order of precedence to look for a match in the ACL entries. The first entry matching a mask is applied to the inbound packet:
	`Console(config)#access-list ip mask-precedence in`
	`Console(config-ip-mask-acl)#mask host any`
	`Console(config-ip-mask-acl)#mask 255.255.255.0 any`
	`Console(config-ip-mask-acl)#`
	Example:
	This shows that the entries in the mask override the precedence in which the rules are entered into the ACL. In the following example, packets with the source address 10.1.1.1 are dropped because the “deny 10.1.1.1 255.255.255.255” rule has the higher precedence according the “mask host any” entry:
	`Console(config)#access-list ip standard A2`
	`Console(config-std-acl)#permit 10.1.1.0 255.255.255.0`
	`Console(config-std-acl)#deny 10.1.1.1 255.255.255.255`
	`Console(config-std-acl)#exit`
	`Console(config)#access-list ip mask-precedence in`
	`Console(config-ip-mask-acl)#mask host any`
	`Console(config-ip-mask-acl)#mask 255.255.255.0 any`
	`Console(config-ip-mask-acl)#`
	Example:
	This shows how to create a standard ACL with an ingress mask to deny access to the IP host 171.69.198.102, and permit access to any others.
	`Console(config)#access-list ip standard A2`
	`Console(config-std-acl)#permit any`
	`Console(config-std-acl)#deny host 171.69.198.102`
	`Console(config-std-acl)#end`
	`Console#show access-list`
	`IP standard access-list A2:`
	`  deny host 171.69.198.102`
	`  permit any`
	`Console#configure`
	`Console(config)#access-list ip mask-precedence in`
	`Console(config-ip-mask-acl)#mask host any`
	`Console(config-ip-mask-acl)#exit`
	`Console(config)#interface ethernet 1/1`
	`Console(config-if)#ip access-group A2 in`
	`Console(config-if)#end`
	`Console#show access-list`
	`IP standard access-list A2:`
	`  deny host 171.69.198.102`
	`  permit any`
	`Console#`

<table>
<tr><th colspan="2">IP ACL Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Function</th></tr>
<tr><td>

mask

(IP ACL - Cont.)

</td><td>

Example:

This shows how to create an extended ACL with an egress mask to drop packets leaving network 171.69.198.0 when the Layer 4 source port is 23

```
Console(config)#access-list ip extended A3
Console(config-ext-acl)#deny host 171.69.198.5 any
Console(config-ext-acl)#deny 171.69.198.0 255.255.255.0 any
source-port 23
Console(config-ext-acl)#end
Console#show access-list
IP extended access-list A3:
  deny host 171.69.198.5 any
  deny 171.69.198.0 255.255.255.0 any source-port 23
Console#config
Console(config)#access-list ip mask-precedence out
Console(config-ip-mask-acl)#mask 255.255.255.0 any source-
port
Console(config-ip-mask-acl)#exit
Console(config)#interface ethernet 1/15
Console(config-if)#ip access-group A3 out
Console(config-if)#end
Console#show access-list
IP extended access-list A3:
  deny 171.69.198.0 255.255.255.0 any source-port 23
  deny host 171.69.198.5 any
IP egress mask ACL:
  mask 255.255.255.0 any source-port
Console#
```

Example:

This is a more comprehensive example. It denies any TCP packets in which the SYN bit is ON, and permits all other packets. It then sets the ingress mask to check the deny rule first, and finally binds port 1 to this ACL.

Note that once the ACL is bound to an interface (i.e., the ACL is active), the order in which the rules are displayed is determined by the associated mask:

```
Switch(config)#access-list ip extended 6
Switch(config-ext-acl)#permit any any
Switch(config-ext-acl)#deny tcp any any control-flag 2 2
Switch(config-ext-acl)#end
Console#show access-list
IP extended access-list A6:
  permit any any
  deny tcp any any control-flag 2 2
Console#configure
Switch(config)#access-list ip mask-precedence in
Switch(config-ip-mask-acl)#mask protocol any any control-flag 2
Switch(config-ip-mask-acl)#end
Console#sh access-list
IP extended access-list A6:
  permit any any
  deny tcp any any control-flag 2 2
IP ingress mask ACL:
  mask protocol any any control-flag 2
Console#configure
Console(config)#interface ethernet 1/1
Console(config-if)#ip access-group A6 in
Console(config-if)#end
Console#show access-list
IP extended access-list A6:
  deny tcp any any control-flag 2 2
  permit any any
IP ingress mask ACL:
  mask protocol any any control-flag 2
Console#
```

</td></tr>
</table>

<table>
<tr><th colspan="2">IP ACL Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Function</th></tr>
<tr><td><b>show access-list ip mask-precedence</b>
This command shows the ingress or egress rule masks for IP ACLs.</td><td><b>Syntax</b>:
<code>show access-list ip mask-precedence [in | out]</code>
• in – Ingress mask precedence for ingress ACLs.
• out – Egress mask precedence for egress ACLs.
<b>Command Mode</b>: Privileged Exec
<b>Example</b>:
<code>Console#show access-list ip mask-precedence</code>
<code>IP ingress mask ACL:</code>
<code> mask host any</code>
<code> mask 255.255.255.0 any</code>
<code>Console#</code></td></tr>
<tr><td><b>ip access-group</b>
This command binds a port to an IP ACL.
Use the no form to remove the port.</td><td><b>Syntax</b>:
<code>[no] ip access-group acl_name in</code>
• acl_name – Name of the ACL. (Maximum length: 16 characters)
• in – Indicates that this list applies to ingress packets.
<b>Default Setting</b>: None
<b>Command Mode</b>: Interface Configuration (Ethernet)
<b>Command Usage</b>: 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. You must configure a mask for an ACL rule before you can bind it to a port.
<b>Example</b>:
<code>Console(config)#int eth 1/25</code>
<code>Console(config-if)#ip access-group david in</code>
<code>Console(config-if)#</code></td></tr>
<tr><td><b>show ip access-group</b>
This command shows the ports assigned to IP ACLs.</td><td><b>Command Mode</b>: Privileged Exec
<b>Example</b>:
<code>Console#show ip access-group</code>
<code>Interface ethernet 1/25</code>
<code> IP standard access-list david</code>
<code>Console#</code></td></tr>
<tr><td><b>map access-list ip</b>
This command sets the output queue for packets matching an ACL rule. The specified CoS value is only used to map the matching packet to an output queue; it is not written to the packet itself.
Use the no form to remove the CoS mapping.</td><td><b>Syntax</b>:
<code>[no] map access-list ip acl_name cos cos-value</code>
• acl_name – Name of the ACL. (Maximum length: 16 characters)
• cos-value – CoS value. (Range: 0-7)
<b>Default Setting</b>: None
<b>Command Mode</b>: Interface Configuration (Ethernet)
<b>Command Usage</b>: A packet matching a rule within the specified ACL is mapped to one of the output queues as shown in the following table. For information on mapping the CoS values to output queues, see queue cos-map on page 4-170.<table><tr><th>Queue</th><th>0</th><th>1</th><th>2</th><th>3</th></tr><tr><td><b>Priority</b></td><td>1,2</td><td>0,3</td><td>4,5</td><td>6,7</td></tr></table><b>Example</b>:
<code>Console(config)#interface ethernet 1/25</code>
<code>Console(config-if)#map access-list ip bill cos 0</code>
<code>Console(config-if)#</code></td></tr>
</table>

IP ACL Commands (Cont.)

Command	Function

show map access-list ip
This command shows the CoS value mapped to an IP ACL for the current interface.
The CoS value determines the output queue for packets matching an ACL rule.
	Syntax:
	`show map access-list ip [interface]`
	• interface
	ethernet unit/port
	unit - This is device 1.
	port - Port number.
	Command Mode: Privileged Exec
	Example:
	`Console#show map access-list ip`
	`Access-list to COS of Eth 1/24`
	` Access-list ALS1 cos 0`
	`Console#`

match access-list ip
This command changes the IEEE 802.1p priority, IP Precedence, or DSCP Priority of a frame matching the defined ACL rule.
This feature is commonly referred to as ACL packet marking.
Use the no form to remove the ACL marker.
	Syntax:
	`match access-list ip acl_name [set priority priority] {set tos tos_value | set dscp dscp_value}`
	`no match access-list ip acl_name`
	• acl_name – Name of the ACL. (Maximum length: 16 characters)
	• priority – Class of Service value in the IEEE 802.1p priority tag. (Range: 0-7; 7 is the highest priority)
	• tos_value – IP Precedence value. (Range: 0-7)
	• dscp_value – Differentiated Services Code Point value. (Range: 0-63)
	Default Setting: None
	Command Mode: Interface Configuration (Ethernet)
	Command Usage: You must configure an ACL mask before you can change frame priorities based on an ACL rule.
	Traffic priorities may be included in the IEEE 802.1p priority tag. This tag is also incorporated as part of the overall IEEE 802.1Q VLAN tag. To specify this priority, use the set priority keywords.
	The IP frame header also includes priority bits in the Type of Service (ToS) octet. The Type of Service octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. To specify the IP precedence priority, use the set tos keywords. To specify the DSCP priority, use the set dscp keywords. Note that the IP frame header can include either the IP Precedence or DSCP priority type.
	The precedence for priority mapping by this switch is IP Precedence or DSCP Priority, and then 802.1p priority.
	Example:
	`Console(config)#interface ethernet 1/12`
	`Console(config-if)#match access-list ip bill set dscp 0`
	`Console(config-if)#`

show marking
This command displays the current configuration for packet marking.
	Command Mode: Privileged Exec
	Example:
	`Console#show marking`
	`Interface ethernet 1/12`
	` match access-list IP bill set DSCP 0`
	` match access-list MAC a set priority 0`
	`Console#`

MAC ACL Commands

MAC ACL Commands	
Command	**Function**

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)
	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 32 rules.
	Example:
	`Console(config)#access-list mac jerry`
	`Console(config-mac-acl)#`

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:
	`[no] {permit | deny}`
	`{any | host source | source address-bitmask}`
	`{any | host destination | destination address-bitmask}`
	`[vid vid [vid-end]] [ethertype protocol [protocol-end]]`
	***Note**: The default is for Ethernet II 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 – Bitmask for MAC address (in hexidecimal format). For all bitmasks, "1" means care and "0" means ignore.
	• vid – VLAN ID. (Range: 1-4094)
	• vid-end – Upper bound of VID range. (Range: 1-4094)
	• protocol – A specific Ethernet protocol number. (Range: 0-65535)
	• protocol-end – Upper bound of protocol range. (Range: 0-65535)
	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)#`

MAC ACL Commands (Cont.)

Command	Function

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 host 00-e0-29-94-34-de ethertype 0800`
	`Console#`

access-list mac mask-precedence
This command changes to MAC Mask mode used to configure access control masks.
Use the no form to delete the mask table.
	Syntax:
	`[no] access-list ip mask-precedence {in | out}`
	• in – Ingress mask for ingress ACLs.
	• out – Egress mask for egress ACLs.
	Default system mask: Filter inbound packets according to specified MAC ACLs.
	Command Mode: Global Configuration
	Command Usage: You must configure a mask for an ACL rule before you can bind it to a port or set the queue or frame priorities associated with the rule.
	A mask can only be used by all ingress ACLs or all egress ACLs.
	The precedence of the ACL rules applied to a packet is not determined by order of the rules, but instead by the order of the masks; i.e., the first mask that matches a rule will determine the rule that is applied to a packet.
	Example:
	`Console(config)#access-list mac mask-precedence in`
	`Console(config-mac-mask-acl)#`

MAC ACL Commands (Cont.)

<table>
<tr><th>Command</th><th>Function</th></tr>
<tr><td>

mask

(MAC ACL)

This command defines a mask for MAC ACLs. This mask defines the fields to check in the packet header.

Use the no form to remove a mask.

</td><td>

Syntax:

```
[no] mask [pktformat]
{any | host | source-bitmask} {any | host | destination-
bitmask}
[vid [vid-bitmask]] [ethertype [ethertype-bitmask]]
```

- pktformat – Check the packet format field. (If this keyword must be used in the mask, the packet format must be specified in ACL rule to match.)
- any – Any address will be matched.
- host – The address must be for a single node.
- source-bitmask – Source address of rule must match this bitmask.
- destination-bitmask – Destination address of rule must match this bitmask.
- vid – Check the VLAN ID field.
- vid-bitmask – VLAN ID of rule must match this bitmask.
- ethertype – Check the Ethernet type field.
- ethertype-bitmask – Ethernet type of rule must match this bitmask.

Default Setting: None

Command Mode: MAC Mask

Command Usage: Up to seven masks can be assigned to an ingress or egress ACL.

Packets crossing a port are checked against all the rules in the ACL until a match is found. The order in which these packets are checked is determined by the mask, and not the order in which the ACL rules were entered.

First create the required ACLs and inbound or outbound masks before mapping an ACL to an interface.

Example:

This example shows how to create an Ingress MAC ACL and bind it to a port. You can then see that the order of the rules have been changed by the mask.

```
Console(config)#access-list mac M4
Console(config-mac-acl)#permit any any
Console(config-mac-acl)#deny tagged-eth2 00-11-11-11-11-11
ff-ff-ff-ff-ff-ff any vid 3
Console(config-mac-acl)#end
Console#show access-list
MAC access-list M4:
  permit any any
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
Console(config)#access-list mac mask-precedence in
Console(config-mac-mask-acl)#mask pktformat ff-ff-ff-ff-ff-ff
any vid
Console(config-mac-mask-acl)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#mac access-group M4 in
Console(config-if)#end
Console#show access-list
MAC access-list M4:
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
  permit any any
MAC ingress mask ACL:
  mask pktformat host any vid
Console#
```

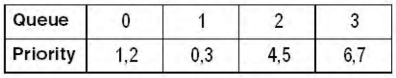
</td></tr>
</table>

MAC ACL Commands (Cont.)	
Command	**Function**

mask (Cont.)	**Example** - This example creates an Egress MAC ACL:
	`Console(config)#access-list mac M5`
	`Console(config-mac-acl)#deny tagged-802.3 host 00-11-11-11-11-11 any`
	`Console(config-mac-acl)#deny tagged-eth2 00-11-11-11-11-11 ff-ff-ff-ff-`
	`ff-ff any vid 3 ethertype 0806`
	`Console(config-mac-acl)#end`
	`Console#show access-list`
	`MAC access-list M5:`
	`  deny tagged-802.3 host 00-11-11-11-11-11 any`
	`  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3 ethertype 0806`
	`Console(config)#access-list mac mask-precedence out`
	`Console(config-mac-mask-acl)#mask pktformat ff-ff-ff-ff-ff-ff any vid`
	`Console(config-mac-mask-acl)#exit`
	`Console(config)#interface ethernet 1/5`
	`Console(config-if)#mac access-group M5 out`
	`Console(config-if)#end`
	`Console#show access-list`
	`MAC access-list M5:`
	`  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3 ethertype 0806`
	`  deny tagged-802.3 host 00-11-11-11-11-11 any`
	`MAC ingress mask ACL:`
	`  mask pktformat host any vid ethertype`
	`Console#`

show access-list mac mask-precedence
This command shows the ingress or egress rule masks for MAC ACLs.
	Syntax:
	`show access-list mac mask-precedence [in | out]`
	• in – Ingress mask precedence for ingress ACLs.
	• out – Egress mask precedence for egress ACLs.
	Command Mode: Privileged Exec
	Example:
	`Console#show access-list mac mask-precedence`
	`MAC egress mask ACL:`
	`  mask pktformat host any vid ethertype`
	`Console#`

permit offset, deny offset
(MAC ACL)
Use this command to add a rule to a MAC ACL. The rule fliters packets matching the specified data pattern starting at the offset.
Use the no form to remove a rule.
	Syntax:
	`{permit | deny} offset offset_value length bitmask data`
	`no {permit | deny} offset offset_value length bitmask data`
	• offset_value – Byte offset from the beginning of the frame.
	• length – Length of the data pattern to match.
	• bitmask – Decimal number representing the data bits to match.
	• data – Data to match, entered as a sequence of hexadecimal letters with no separators.
	Default Setting: None
	Command Mode: MAC ACL
	Command Usage: This command is used to filter frames that match a specified pattern, and can be used to filter traffic associated with precisely defined events.
	The bitmask is a decimal number (representing an equivalent bit mask) that is applied to the data. Enter a decimal number, where the equivalent binary bit “1” means to match a bit and “0” means to ignore a bit.
	Packet filtering based on arbitrary offsets and data patterns can adversely affect switch throughput. Try to avoid using packet filtering based on pattern matching unless this is absolutely necessary to solve a specific problem.
	Example:
	This example shows how to filter any Ethernet II packets directed to the IP address 10.1.0.23 that have the *Don’t Fragment* flag set.
	`Console(config)#access-list mac jerry`
	`Console(config-mac-acl)#permit offset ???`

<table>
<tr><th colspan="2">MAC ACL Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Function</th></tr>
<tr><td><b>mac access-group</b>
This command binds a port to a MAC ACL.
Use the no form to remove the port.</td><td><b>Syntax</b>:
mac access-group acl_name in
• acl_name – Name of the ACL. (Maximum length: 16 characters)
• in – Indicates that this list applies to ingress packets.
<b>Default Setting</b>: None
<b>Command Mode</b>: Interface Configuration (Ethernet)
<b>Command Usage</b>: 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.
<b>Example</b>:
Console(config)#interface ethernet 1/25
Console(config-if)#mac access-group alexander in
Console(config-if)#</td></tr>
<tr><td><b>show mac access-group</b>
This command shows the ports assigned to MAC ACLs.</td><td><b>Command Mode</b>: Privileged Exec
<b>Example</b>:
Console#show mac access-group
Interface ethernet 1/5
 MAC access-list M5 in
Console#</td></tr>
<tr><td><b>map access-list mac</b>
This command sets the output queue for packets matching an ACL rule.
The specified CoS value is only used to map the matching packet to an output queue; it is not written to the packet itself.
Use the no form to remove the CoS mapping.</td><td><b>Syntax</b>:
[no] map access-list mac acl_name cos cos-value
• acl_name – Name of the ACL. (Maximum length: 16 characters)
• cos-value – CoS value. (Range: 0-7)
<b>Default Setting</b>: None
<b>Command Mode</b>: Interface Configuration (Ethernet)
<b>Command Usage</b>: You must configure an ACL mask before you can map CoS values to the rule.
A packet matching a rule within the specified ACL is mapped to one of the output queues as shown below:

<table>
<tr><th>Queue</th><th>0</th><th>1</th><th>2</th><th>3</th></tr>
<tr><td>Priority</td><td>1,2</td><td>0,3</td><td>4,5</td><td>6,7</td></tr>
</table>
<b>Example</b>:
Console(config)#int eth 1/5
Console(config-if)#map access-list mac M5 cos 0
Console(config-if)#</td></tr>
<tr><td><b>show map access-list mac</b>
This command shows the CoS value mapped to a MAC ACL for the current interface.
The CoS value determines the output queue for packets matching an ACL rule.</td><td><b>Syntax</b>:
show map access-list mac [interface]
• interface
ethernet unit/port
   unit - This is device 1.
   port - Port number.
<b>Command Mode</b>: Privileged Exec
<b>Example</b>:
Console#show map access-list mac
Access-list to COS of Eth 1/5
 Access-list M5 cos 0
Console#</td></tr>
</table>

MAC ACL Commands (Cont.)

Command	Function

match access-list mac
This command changes the IEEE 802.1p priority of a Layer 2 frame matching the defined ACL rule.
This feature is commonly referred to as ACL packet marking.
Use the no form to remove the ACL marker.
	Syntax:
	`match access-list mac acl_name set priority priority`
	`no match access-list mac acl_name`
	• acl_name – Name of the ACL. (Maximum length: 16 characters)
	• priority – Class of Service value in the IEEE 802.1p priority tag. (Range: 0-7; 7 is the highest priority)
	Default Setting: None
	Command Mode: Interface Configuration (Ethernet)
	Command Usage: You must configure an ACL mask before you can change frame priorities based on an ACL rule.
	Example:
	`Console(config)#interface ethernet 1/12`
	`Console(config-if)#match access-list mac a set priority 0`
	`Console(config-if)#`

show marking	Displays the current configuration for packet marking

ACL Information

ACL Information

Command	Function

show access-list
This command shows all ACLs and associated rules, as well as all the user-defined masks.
	Command Mode: Privileged Exec
	Command Usage: Once the ACL is bound to an interface (i.e., the ACL is active), the order in which the rules are displayed is determined by the associated mask.
	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 0.0.0.255 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`
	`IP ingress mask ACL:`
	`  mask protocol any any control-flag 2`
	`Console#`

show access-group
This command shows the port assignments of ACLs.
	Command Mode: Privileged Executive
	Example:
	`Console#show access-group`
	`Interface ethernet 1/25`
	` IP standard access-list david`
	` MAC access-list jerry`
	`Console#`

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.

SNMPv3 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 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>
<tr><th colspan="2">SNMP Commands</th></tr>
<tr><th>Command</th><th>Function</th></tr>
<tr><td>

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.

</td><td>

Default Setting: Enabled

Command Mode: Global Configuration

Example:

```
Console(config)#snmp-server
Console(config)#
```

</td></tr>
<tr><td>

show snmp

This command checks the status of SNMP communications.

</td><td>

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

System Contact: Joe
System Location: Room 23

SNMP traps:
 Authentication: enabled
 Link-up-down:   enabled

SNMP communities:
   1. private, and the privilege is read-write
   2. public, and the privilege is read-only

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#
```

</td></tr>
</table>

SNMP Commands (Cont.)

Command	**Function**

snmp-server community
This command defines the community access string for the Simple Network Management Protocol.
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 Settings:
	• 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
	Command Usage: The first snmp-server community command you enter enables SNMP (SNMPv1). The no snmp-server community command disables SNMP.
	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)#`

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)#`

SNMP Commands (Cont.)

Command	Function

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 community-string [version {1 | 2c}]`
	`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)
	• community-string - Password-like community string sent with the notification operation. Although you can set this string using the snmp-server host command by itself, we recommend that you define this string using 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 v1 or v2c traps.
	Default Settings:
	• Host Address: None
	• SNMP Version: 1
	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 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.
	The switch can send SNMP version 1 or version 2c 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.
	Example:
	`Console(config)#snmp-server host 10.1.19.23 batman`
	`Console(config)#`

snmp-server enable traps
This command enables this device to send Simple Network Management Protocol traps (SNMP notifications).
Use the no form to disable SNMP notifications.
	Syntax:
	`[no] snmp-server enable traps [authentication | link-up-down]`
	• authentication - Keyword to issue authentication failure traps.
	• link-up-down - Keyword to issue link-up or link-down traps.
	***Note**: The link-up-down trap can only be enabled/disabled via the CLI.*
	Default Setting: Issue authentication and link-up-down 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.
	Example:
	`Console(config)#snmp-server enable traps link-up-down`
	`Console(config)#`

SNMP Commands (Cont.)

Command	**Function**

snmp-server engine-id
Use this command to configure an identification string for the SNMP v3 engine.
Use the no form to restore the default.
	Syntax:
	`snmp-server engine-id local engineid-string`
	`no snmp-server engine-id local`
	• 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 on this 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.
	Trailing zeroes need not be entered to uniquely specify a engine ID. In other words, the value “1234” is equivalent to “1234” followed by 22 zeroes.
	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 engineID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users (page 112).
	Example:
	`Console(config)#snmp-server engineID local 12345`
	`Console(config)#`

show snmp engine-id
Use this command to show 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`
	• Local SNMP engineID: String identifying the engine ID.
	• Local SNMP engineBoots: The number of times that the engine has (re-)initialized since the snmpEngineID was last configured.

snmp-server view
Use this command to add an SNMP view that 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: 1-64 characters)
	• oid-tree - Object identifier of a branch within the MIB tree. Wildcards 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.
	Example: This view includes MIB-2:
	`Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included`
	`Console(config)#`
	Example: This view includes the MIB-2 interfaces table, ifDescr. The wildcard 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)#`
	Example: 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)#`

SNMP Commands (Cont.)

Command	**Function**

show snmp view
Use this command to show information on the SNMP groups.
	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: nonvolatile`
	`Row Status: active`
	
	`View Name: defaultview`
	`Subtree OID: 1`
	`View Type: included`
	`Storage Type: nonvolatile`
	`Row Status: active`
	
	`Console#`
	• 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 group
Use this command to add 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]`
	`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.
	• readview - Defines the view for read access. (1-64 characters)
	• writeview - Defines the view for write access. (1-64 characters)
	Default Settings:
	• readview - Every object belonging to the Internet OID space (1.3.6.1).
	• writeview - 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.
	Example:
	`Console(config)#snmp-server group r&d v3 auth write daily`
	`Console(config)#`

SNMP Commands (Cont.)

Command	**Function**

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`
	`Security Model: v3`
	`Read View: defaultview`
	`Write View: daily`
	`Notify View: none`
	`Storage Type: nonvolatile`
	`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#`
	• groupname: Name of an SNMP group.
	• security model: The SNMP version.
	• readview: The associated read view.
	• writeview: The associated write view.
	• notifyview: The associated notify view.
	• storage-type: The storage type for this entry.
	• Row Status: The row status of this entry.

SNMP Commands (Cont.)

Command	**Function**

snmp-server user
Use this command to add a user to an SNMP group, restricting the user to a specific SNMP Read and a Write View.
Use the no form to remove a user from an SNMP group.
	Syntax:
	`snmp-server user username groupname {v1 | v2c | v3 [encrypted] [auth {md5 | sha} auth-password [priv des56 priv-password]]`
	`no snmp-server user username`
	• 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)
	• 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 56-bit DES data 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: 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.
	SNMP passwords are localized using the authoritative SNMP engine ID.
	Example:
	`Console(config)#snmp-server user steve group r&d v3 auth md5 greenpeace priv des56 einstien`
	`Console(config)#`

show snmp user
Use this command to show information on SNMP users.
	Command Mode: Privileged Exec
	Example:
	`Console#show snmp user`
	`EngineId: 01000000000000000000000000`
	`User Name: steve`
	`Authentication Protocol: md5`
	`Privacy Protocol: des56`
	`Storage Type: nonvolatile`
	`Row Status: active`
	
	`Console#`
	• 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.

Interface Commands

These commands are used to display or set communication parameters for an Ethernet port, aggregated link, or VLAN.

Interface Commands

Command	**Function**

interface
This command configures an interface type and enter interface configuration mode.
Use the no form to remove a trunk.
	Syntax:
	`interface interface`
	`no interface port-channel channel-id`
	• interface
	ethernet unit/port
	unit - Stack unit. (Range: 1-8)
	port - Port number. (Range: 1-26)
	• port-channel channel-id (Range: 1-4)
	• vlan vlan-id (Range: 1-4094)
	Default Setting: None
	Command Mode: Global Configuration
	Example: To specify port 24, enter the following command:
	`Console(config)#interface ethernet 1/24`
	`Console(config-if)#`

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)
	Example: The following example adds a description to port 24:
	`Console(config)#interface ethernet 1/24`
	`Console(config-if)#description RD-SW#3`
	`Console(config-if)#`

speed-duplex
This command configures the speed and duplex mode of a given interface when autonegotiation is disabled.
Use the no form to restore the default.
	Syntax:
	`speed-duplex {1000full | 100full | 100half | 10full | 10half}`
	`no speed-duplex`
	• 1000full - Forces 1000 Mbps full-duplex operation
	• 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 100half for 100BASE-TX ports and 1000full for Gigabit Ethernet ports.
	Command Mode: Interface Configuration (Ethernet, Port Channel)
	Command Usage: 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)#`

Interface Commands (Cont.)

Command	Function

negotiation
This command enables autonegotiation for a given interface.
Use the no form to disable autonegotiation.
	Syntax:
	`[no] negotiation`
	Default Setting: Enabled
	Command Mode: Interface Configuration (Ethernet, Port Channel)
	Command Usage: 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 autonegotiation is disabled, auto-MDI/MDI-X pin signal configuration will also be disabled for the RJ-45 ports.
	Example: The following example configures port 11 to use autonegotiation:
	`Console(config)#interface ethernet 1/11`
	`Console(config-if)#negotiation`
	`Console(config-if)#`

capabilities
This command advertises the port capabilities of a given interface during autonegotiation.
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 1000 Mbps 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; when not specified, the port will auto-negotiate to determine the sender and receiver for asymmetric pause frames. (The current switch ASIC only supports symmetric pause frames.)
	Default Settings:
	• 100BASE-TX: 10half, 10full, 100half, 100full
	• 1000BASE-T: 10half, 10full, 100half, 100full, 1000full
	• SFP: 1000full
	Command Mode: Interface Configuration (Ethernet, Port Channel)
	Command Usage: 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 100half, 100full and flow control:
	`Console(config)#interface ethernet 1/5`
	`Console(config-if)#capabilities 100half`
	`Console(config-if)#capabilities 100full`
	`Console(config-if)#capabilities flowcontrol`
	`Console(config-if)#`

Interface Commands (Cont.)

Command	Function

flowcontrol
This command enables flow control.
Use the no form to disable flow control.
	Syntax:
	`[no] flowcontrol`
	Default Setting: Flow control enabled
	Command Mode: Interface Configuration (Ethernet, Port Channel)
	Command Usage: 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 802.3x 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)#`

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)#`

switchport broadcast packet-rate
This command configures broadcast storm control.
Use the no form to disable broadcast storm control.
	Syntax:
	`switchport broadcast octet-rate rate`
	`no switchport broadcast`
	• rate - Threshold level as a rate; i.e., octets per second. (Range: 64-95232000)
	Default Setting: Enabled for all ports
	Packet-rate limit: 32000 octets per second
	Command Mode: Interface Configuration (Ethernet)
	Command Usage: When broadcast traffic exceeds the specified threshold, packets above that threshold are dropped.
	This command can enable or disable broadcast storm control for the selected interface. However, the specified threshold value applies to all ports on the switch.
	Example: The following shows how to configure broadcast storm control at 600 packets per second:
	`Console(config)#interface ethernet 1/5`
	`Console(config-if)#switchport broadcast octet-rate 600`
	`Console(config-if)#`

Interface Commands (Cont.)

Command | **Function**

clear counters

This command clears statistics on an interface.

Syntax:

```
clear counters interface
```

- interface

  ethernet unit/port

  unit - Stack unit. (Range: 1-8)

  port - Port number. (Range: 1-26)

- port-channel channel-id (Range: 1-4)

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 status

This command displays the status for an interface.

Syntax:

```
show interfaces status [interface]
```

- interface

  ethernet unit/port

  unit - Stack unit. (Range: 1-8)

  port - Port number. (Range: 1-26)

- port-channel channel-id (Range: 1-4)
- vlan vlan-id (Range: 1-4094)

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 - CLI* on page 86.

Example:

```
Console#show interfaces status ethernet 1/5
Information of Eth 1/5
 Basic information:
  Port type:                100TX
  Mac address:              00-00-AB-CD-00-01
 Configuration:
  Name:
  Port admin:               Up
  Speed-duplex:             Auto
  Capabilities:             10half, 10full, 100half, 100full,
  Broadcast storm:          Enabled
  Broadcast storm limit:    32000 octets/second
  Flow control:             Disabled
  Lacp:                     Disabled
  Port security:            Disabled
  Max MAC count:            0
  Port security action:     None
 Current status:
  Link status:              Up
  Port operation status:    Up
  Operation speed-duplex:   100full
  Flow control type:        None
Console#show interfaces status vlan 1
 Information of VLAN 1
 MAC address:               00-00-AB-CD-00-00
Console#
```

Interface Commands (Cont.)

Command	**Function**

show interfaces counters
This command displays interface statistics.
	Syntax:
	`show interfaces counters [interface]`
	• interface
	ethernet unit/port
	unit - Stack unit. (Range: 1-8)
	port - Port number. (Range: 1-26)
	• port-channel channel-id (Range: 1-4)
	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 *Port Statistics* on page 100.
	Example:
	`Console#show interfaces counters ethernet 1/7`
	`Ethernet 1/7`
	` Iftable stats:`
	`  Octets input: 30658, Octets output: 196550`
	`  Unicast input: 6, Unicast output: 5`
	`  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: 0, Multi-cast output: 3064`
	`  Broadcast input: 262, Broadcast output: 1`
	` 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`
	`  Frame too longs: 0, Carrier sense errors: 0`
	`  Symbol errors: 0`
	` RMON stats:`
	`  Drop events: 0, Octets: 227208, Packets: 3338`
	`  Broadcast pkts: 263, Multi-cast pkts: 3064`
	`  Undersize pkts: 0, Oversize pkts: 0`
	`  Fragments: 0, Jabbers: 0`
	`  CRC align errors: 0, Collisions: 0`
	`  Packet size <= 64 octets: 3150, Packet size 65 to 127 octets: 139`
	`  Packet size 128 to 255 octets: 49, Packet size 256 to 511 octets: 0`
	`  Packet size 512 to 1023 octets: 0, Packet size 1024 to 1518 octets: 0`
	`Console#`

<table>
<tr><th colspan="2">Interface Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Function</th></tr>
<tr>
<td><b>show interfaces switchport</b>
This command displays the administrative and operational status of the specified interfaces.</td>
<td><b>Syntax</b>:
<pre>show interfaces switchport [interface]</pre>
• interface
ethernet unit/port
unit - Stack unit. (Range: 1-8)
port - Port number. (Range: 1-26)
• port-channel channel-id (Range: 1-4)
<b>Default Setting</b>: Shows all interfaces.
<b>Command Mode</b>: Normal Exec, Privileged Exec
<b>Command Usage</b>: If no interface is specified, information on all interfaces is displayed.
<b>Example</b>: This example shows the configuration setting for port 24:
<pre>Console#show interfaces switchport ethernet 1/24
 Broadcast threshold: Enabled, 600 octets/second
 LACP status: Enabled
 Ingress rate limit: disable, Level: 30
 Egress rate limit: disable, Level: 30
 VLAN membership mode: Hybrid
 Ingress rule: Disabled
 Acceptable frame type: All frames
 Native VLAN: 1
 Priority for untagged traffic: 0
 Gvrp status: Disabled
 Allowed Vlan: 1(u),
 Forbidden Vlan:
 Private-VLAN mode: NONE
 Private-VLAN host-association: NONE
 Private-VLAN mapping: NONE
Console#</pre>
<b>Interfaces Switchport Statistics</b>
• Broadcast threshold: Shows if broadcast storm suppression is enabled or disabled; if enabled it also shows the threshold level (see <i>switchport broadcast packet-rate</i> on page 233).
• Lacp status: Shows if Link Aggregation Control Protocol has been enabled or disabled (see <i>lacp</i> on page 240).
• Ingress/Egress rate limit: Shows if rate limiting is enabled, and the current rate limit. (see <i>rate-limit</i> on page 238).
• VLAN membership mode: Indicates membership mode as Trunk or Hybrid (see <i>switchport mode</i> on page 256).
• Ingress rule: Shows if ingress filtering is enabled or disabled (see <i>switchport ingress-filtering</i> on page 257).
• Acceptable frame type: Shows if acceptable VLAN frames include all types or tagged frames only (see <i>switchport acceptable-frame-types</i> on page 256).
• Native VLAN: Indicates the default Port VLAN ID (see <i>switchport native vlan</i> on page 257).
• Priority for untagged traffic: Indicates the default priority for untagged frames (see <i>Priority Commands</i> on page 264).
• Gvrp status: Shows if GARP VLAN Registration Protocol is enabled or disabled (see <i>switchport gvrp</i> on page 258).
• Allowed Vlan: Shows the VLANs this interface has joined, where “(u)” indicates untagged and “(t)” indicates tagged (see <i>switchport allowed vlan</i> on page 258).
• Forbidden Vlan: Shows the VLANs this interface can not dynamically join via GVRP (see <i>switchport forbidden vlan</i> on page 258).
• Private VLAN mode: Shows the private VLAN mode as host, promiscuous, or none (see <i>switchport mode private-vlan</i> on page 261).
• Private VLAN host-association: Shows the secondary (or community) VLAN with which this port is associated (see <i>switchport private-vlan host-association</i> on page 261).
• Private VLAN mapping: Shows the primary VLAN mapping for a promiscuous port (see <i>switchport private-vlan mapping</i> on page 261).</td>
</tr>
</table>

Mirror Port Commands

This section describes how to mirror traffic from a source port to a target port.

Mirror Port Commands

Command	Function

port monitor
This command configures a mirror session.
Use the no form to clear a mirror session.
	Syntax:
	`port monitor interface [rx │ tx]`
	`no port monitor interface`
	• interface - ethernet unit/port (source port)
	• unit - Stack unit. (Range: 1-8)
	• port - Port number. (Range: 1-26)
	• rx - Mirror received packets.
	• tx - Mirror transmitted packets.
	Default Setting: No mirror session is defined.
	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.
	• The destination port is set by specifying an Ethernet interface.
	• The mirror port and monitor port speeds should match, otherwise traffic may be dropped from the monitor port.
	You can create multiple mirror sessions, but all sessions must share the same destination port. However, you should avoid sending too much traffic to the destination port from multiple source ports.
	Example: The following example configures the switch to mirror received packets from port 6 to 11:
	`Console(config)#interface ethernet 1/11`
	`Console(config-if)#port monitor ethernet 1/6 rx`
	`Console(config-if)#`

show port monitor
This command displays mirror information.
	Syntax: show port monitor [interface]
	• interface - ethernet unit/port (source port)
	• unit - Stack unit. (Range: 1-8)
	• port - Port number. (Range: 1-26)
	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).
	Example: The following shows mirroring configured from port 6 to port 11:
	`Console(config)#interface ethernet 1/11`
	`Console(config-if)#port monitor ethernet 1/6 rx`
	`Console(config-if)#end`
	`Console#show port monitor`
	`Port Mirroring`
	`-------------------------------------`
	` Destination port(listen port):Eth1/11`
	` Source port(monitored port)  :Eth1/6`
	` Mode                         :RX`
	`Console#`

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. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. 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.

Rate Limit Commands

Command	Function

rate-limit
Use this command to define the rate limit level for a specific interface.
Use this command without specifying a rate to restore the default rate limit level.
Use the no form to restore the default status of disabled.
	Syntax:
	`rate-limit {input | output} level [rate]`
	`no rate-limit {input | output}`
	• input – Input rate
	• output – Output rate
	• rate – Maximum value in Mbps. (Range: 1-30)
	Default Settings:
	• Fast Ethernet interface – 100 Mbps
	• Gigabit Ethernet interface – 1000 Mbps
	Command Mode: Interface Configuration (Ethernet, Port Channel)
	Command Usage:
	The range is:
	• Fast Ethernet interface – 1 to 100 Mbps
	• Gigabit Ethernet interface – 8 to 1000 Mbps
	Resolution – The increment of change:
	• Fast Ethernet interface – 1 Mbps
	• Gigabit Ethernet interface – 8 Mbps
	Example:
	`Console(config)#interface ethernet 1/1`
	`Console(config-if)#rate-limit input level 20`
	`Console(config-if)#`

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 six trunks. For example, a trunk consisting of two 1000 Mbps ports can support an aggregate bandwidth of 4 Gbps when operating at full duplex.

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 eight 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, duplex mode and flow control), VLAN assignments, and CoS settings.
- 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.

Link Aggregation Commands	
Command	**Function**
Manual Configuration Commands	
interface port-channel	See page 231.

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: 1-4)
	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 interfaces port-channel to remove a trunk from the switch.
	Example: The following example creates trunk 1 and then adds port 11:
	`Console(config)#interface port-channel 1`
	`Console(config-if)#exit`
	`Console(config)#interface ethernet 1/11`
	`Console(config-if)#channel-group 1`
	`Console(config-if)#`

<table>
<tr><th colspan="2">Link Aggregation Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Function</th></tr>
<tr><td colspan="2"><b>Dynamic Configuration Commands</b></td></tr>
<tr>
<td>

lacp

This command enables 802.3ad Link Aggregation Control Protocol (LACP) for the current interface.

Use the no form to disable it.

</td>
<td>

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 11-13. 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 Trunk 1 has been established:

```
Console(config)#interface ethernet 1/11
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/13
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#exit
Console#show interfaces status port-channel 1
Information of Trunk 1
 Basic information:
  Port type:                100TX
  Mac address:              00-00-e8-00-00-0b
 Configuration:
  Name:
  Port admin:               Up
  Speed-duplex:             Auto
  Capabilities:             10half, 10full, 100half, 100full
  Flow control status:      Disabled
  Port security:            Disabled
  Max MAC count:            0
 Current status:
  Created by:               LACP
  Link status:              Up
  Operation speed-duplex:   100full
  Flow control type:        None
  Member Ports: Eth1/11, Eth1/12, Eth1/13,
Console#
```

</td>
</tr>
</table>

Link Aggregation Commands (Cont.)

Command	**Function**

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
(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)#`

<table>
<tr><th colspan="2">Link Aggregation Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Function</th></tr>
<tr><td><b>lacp admin-key</b>
<b>(Port Channel)</b>
This command configures a port channel's LACP administration key string.
Use the no form to restore the default setting.</td><td><b>Syntax</b>:
lacp {actor | partner} admin-key key
[no] lacp {actor | partner} 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)
<b>Default Setting</b>: 0
<b>Command Mode</b>: Interface Configuration (Port Channel)
<b>Command Usage</b>: 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.
<b>Example</b>:
Console(config)#interface port-channel 1
Console(config-if)#lacp actor admin-key 3
Console(config-if)#</td></tr>
<tr><td><b>lacp port-priority</b>
This command configures LACP port priority.
Use the no form to restore the default setting.</td><td><b>Syntax</b>:
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)
<b>Default Setting</b>: 32768
<b>Command Mode</b>: Interface Configuration (Ethernet)
<b>Command Usage</b>: 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.
<b>Example</b>:
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor port-priority 128</td></tr>
</table>

<table>
<tr><th colspan="2">Link Aggregation Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Function</th></tr>
<tr><td colspan="2"><b>Trunk Status Display Command</b></td></tr>
<tr><td><b>show interfaces status port-channel</b></td><td>Shows trunk information</td></tr>
<tr><td><b>show lacp</b>
This command displays LACP information.</td><td><b>Syntax</b>:
<pre>
show lacp [port-channel] {counters | internal | neighbors |
sysid}
</pre>
• port-channel - Local identifier for a link aggregation group. (Range: 1-4)
• counters - Statistics for LACP protocol messages.
• internal - Configuration settings and operational state for local side.
• neighbors - Configuration settings and operational state for remote side.
• sysid - Summary of system priority and MAC address for all channel groups.
<b>Default Setting</b>: Port Channel: all
<b>Command Mode</b>: Privileged Exec
<b>Example</b>:
<pre>
Console#show 1 lacp counters
Channel group : 1 ---
Eth 1/ 1 ---
  LACPDUs Sent : 21
  LACPDUs Received : 21
  Marker Sent : 0
  Marker Received : 0
  LACPDUs Unknown Pkts : 0
  LACPDUs Illegal Pkts : 0
.
.
.
</pre>
• 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.</td></tr>
</table>

Link Aggregation Commands (Cont.)

Command	Function
show lacp (Cont.)	**Example**:

```
Console#show lacp 1 internal
Channel group : 1
-------------------------------------------------------------
------------
Oper Key : 4
Admin Key : 0
Eth 1/1
-------------------------------------------------------------
------------
  LACPDUs Internal : 30 sec
  LACP System Priority : 32768
  LACP Port Priority : 32768
  Admin Key : 4
  Oper Key : 4
  Admin State : defaulted, aggregation, long timeout, LACP-
activity
  Oper State : distributing, collecting, synchronization,
aggregation,
               long timeout, LACP-activity
.
.
.
```

- 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.
- 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)

<table>
<tr><th colspan="2">Link Aggregation Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Function</th></tr>
<tr><td>

show lacp (Cont.)

</td><td>

Example:

```
Console#show lacp 1 neighbors
Channel group 1 neighbors
------------------------------------------------------------
------------
Eth 1/1
------------------------------------------------------------
------------
  Partner Admin System ID : 32768, 00-00-00-00-00-00
  Partner Oper System ID : 32768, 00-00-00-00-00-01
  Partner Admin Port Number : 1
  Partner Oper Port Number : 1
  Port Admin Priority : 32768
  Port Oper Priority : 32768
  Admin Key : 0
  Oper Key : 4
  Admin State : defaulted, distributing, collecting,
synchronization,
                long timeout,
  Oper State : distributing, collecting, synchronization,
aggregation,
               long timeout, LACP-activity
.
.
.
```

- 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.)

Example:

```
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
Console#
```

- 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.

***Note**: The LACP system priority and system MAC address are concatenated to form the LAG system ID.*

</td></tr>
</table>

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.

Address Table Commands	
Command	**Function**

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 - Stack unit. (Range: 1-8)
	port - Port number. (Range: 1-26)
	port-channel *channel-id* (Range: 1-4)
	• 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`

clear mac-address-table dynamic This command removes any learned entries from the forwarding database and clears the transmit and receive counts for any static or system configured entries.	**Default Setting**: None **Command Mode**: Privileged Exec **Example**: `Console#clear mac-address-table dynamic`

Address Table Commands (Cont.)

Command	Function
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 - Stack unit. (Range: 1-8) port - Port number. (Range: 1-26) port-channel *channel-id* (Range: 1-4) • 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.

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: 10-30000 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)#`

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 time: 100 sec.`
	`Console#`

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.

Spanning Tree Commands	
Command	**Function**

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 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}`
	`no spanning-tree mode`
	• stp - Spanning Tree Protocol (IEEE 802.1D)
	• rstp - Rapid Spanning Tree Protocol (IEEE 802.1w)
	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.
	• 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.
	Example: The following example configures the switch to use Rapid Spanning Tree:
	`Console(config)#spanning-tree mode rstp`
	`Console(config)#`

Spanning Tree Commands (Cont.)

Command	Function

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.
	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)`

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)#`

Spanning Tree Commands (Cont.)	
Command	**Function**

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 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 40960`
	`Console(config)#`

spanning-tree pathcost method
This command configures the path cost method used for Rapid 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 0-200,000,000.
	• short - Specifies 16-bit based values that range from 0-65535.
	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 (see *spanning-tree cost* on page 251) takes precedence over port priority (see *spanning-tree port-priority* on page 251).
	Example:
	`Console(config)#spanning-tree pathcost method long`
	`Console(config)#`

spanning-tree transmission-limit
This command configures the minimum interval between the transmission of consecutive RSTP 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)#`

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 Commands (Cont.)

Command	Function

spanning-tree cost
This command configures the spanning tree path cost for the specified interface.
Use the no form to restore the default.
	Syntax:
	`spanning-tree cost cost`
	`no spanning-tree cost`
	• cost - The path cost for the port. (Range: 1-200,000,000))
	The recommended range is:
	Ethernet: 200,000-20,000,000
	Fast Ethernet: 20,000-2,000,000
	Gigabit Ethernet: 2,000-200,000
	Default Settings:
	• 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
	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.
	Note: *Path cost takes precedence over port priority.*
	When the spanning-tree pathcost method (page 4-141) 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 5000`
	`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 the lowest numeric identifier will be enabled.
	Example:
	`Console(config)#interface ethernet 1/5`
	`Console(config-if)#spanning-tree port-priority 128`

Spanning Tree Commands (Cont.)

Command	Function

spanning-tree edge-port
This command specifies an interface as an edge port.
Use the no form to restore the default.
	Syntax:
	`[no] spanning-tree 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 timeout 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.
	Example:
	`Console(config)#interface ethernet ethernet 1/5`
	`Console(config-if)#spanning-tree edge-port`
	`Console(config-if)#`

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)#spanning-tree portfast`
	`Console(config-if)#`

Spanning Tree Commands (Cont.)

Command	Function

spanning-tree link-type
This command configures the link type for Rapid 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.
	Example:
	`Console(config)#interface ethernet 1/5`
	`Console(config-if)#spanning-tree link-type point-to-point`

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 - Stack unit. (Range: 1-8)
	port - Port number. (Range: 1-26)
	port-channel channel-id (Range: 1-6)
	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 ethernet 1/5`
	`Console#`

<table>
<tr><th colspan="2">Spanning Tree Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Function</th></tr>
<tr><td>

show spanning-tree

This command shows the configuration for the spanning tree.

</td><td>

Syntax:

```
show spanning-tree [interface]
```

- interface

  ethernet unit/port

    unit - Stack unit. (Range: 1-8)

    port - Port number. (Range: 1-26)

  port-channel channel-id (Range: 1-4)

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 and for every interface in the tree.

Use the show spanning-tree interface command to display the spanning tree configuration for a specific interface.

For a description of the items displayed under “Spanning-tree information,” see *Configuring Global Settings* on page 115.

For a description of the items displayed for specific interfaces, see *Displaying Interface Settings* on page 118.

Example:

```
Console#show spanning-tree
Spanning-tree information
--------------------------------------------------------------
-
 Spanning tree mode:               RSTP
 Spanning tree enabled/disabled:   enabled
 Priority:                         40960
 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
 Designated Root:                  32768.0.0000ABCD0000
 Current root port:                1
 Current root cost:                50000
 Number of topology changes:       5
 Last topology changes time (sec.):226
 Transmission limit:               3
 Path Cost Method:                 long
--------------------------------------------------------------
-
Eth  1/ 1 information
--------------------------------------------------------------
-
Admin status:          enabled
 Role:                 root
 State:                forwarding
 Path cost:            100000
 Priority:             128
 Designated cost:      200000
 Designated port:      128.24
 Designated root:      32768.0.0000ABCD0000
 Designated bridge:    32768.0.0030F1552000
 Fast forwarding:      enabled
 Forward transitions:  1
 Admin edge port:      enabled
 Oper edge port:       disabled
 Admin Link type:      auto
 Oper Link type:       point-to-point
 Spanning Tree Status: enabled
.
.
.
Console#
```

</td></tr>
</table>

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.

Editing VLAN Groups

Editing VLAN Groups	
Command	**Function**

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)#`

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 - ID of 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.
	• 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.
	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)#`

Configuring VLAN Interfaces

Configuring VLAN Interfaces	
Command	**Function**

interface vlan
This command enters interface configuration mode for VLANs, which is used to configure VLAN parameters for a physical interface.
	Syntax:
	`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)#`

switchport mode
This command configures the VLAN membership mode for a port. Use the no form to restore the default.
	Syntax:
	`switchport mode {trunk | hybrid | private-vlan}`
	`no switchport mode`
	• 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.
	• hybrid - Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.
	• private-vlan - For an explanation of this command see *switchport mode private-vlan* on page 261.
	Default Setting: All ports are in hybrid mode with the PVID set to VLAN 1.
	Command Mode: Interface Configuration (Ethernet, Port Channel)
	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)#`

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)#`

Configuring VLAN Interfaces (Cont.)	
Command	**Function**

switchport ingress-filtering
This command enables ingress filtering for an interface.
Use the no form to restore the default.
	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 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: If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.
	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)#`

Configuring VLAN Interfaces (Cont.)

Command	Function

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 gvrp	See page 263.

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 priority default	Sets a port priority for incoming untagged frames

Displaying VLAN Information

Displaying VLAN Information	
Command	**Function**

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 “show vlan private-vlan” on page 4-162
	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`
	
	`Vlan ID:                1`
	`Type:                   Static`
	`Name:                   DefaultVlan`
	`Status:                 Active`
	`Ports/Port channel:  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)`
	
	`Console#`

show interfaces status vlan	See page 234.
show interfaces switchport	See page 236

Configuring Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. This switch supports two types of private VLAN ports: promiscuous, and community ports.

- A promiscuous port can communicate with all interfaces within a private VLAN.
- Community ports can only communicate with other ports in their own community VLAN, and with their designated promiscuous ports.

This section describes commands used to configure private VLANs.

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 the community groups.
2. Use the **private-vlan association** command to map the secondary (i.e., 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., having access restricted to community VLAN members, and channeling all other traffic through a promiscuous port).
4. Use the **switchport private-vlan host-association** command to assign a port to a secondary 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.

Edit Private VLAN Groups

<table>
<tr><th colspan="2">Edit Private VLAN Groups</th></tr>
<tr><th>Command</th><th>Function</th></tr>
<tr><td><b>private-vlan</b>
Use this command to create a primary, isolated or community private VLAN.
Use the no form to remove the specified private VLAN.</td><td><b>Syntax</b>:
private-vlan vlan-id {community | primary | isolated}
no private-vlan vlan-id
• vlan-id - ID of private VLAN. (Range: 1-4094, no leading zeroes).
• community - A VLAN in which traffic is restricted to port members.
• primary - A VLAN which can contain one or more community VLANs, and serves to channel traffic between community VLANs and other locations.
• isolated – Specifies an isolated VLAN. Ports assigned to an isolated VLAN can only communicate with promiscuous ports within their own VLAN.
<b>Default Setting</b>: None
<b>Command Mode</b>: VLAN Configuration
<b>Command Usage</b>: Private VLANs are used to restrict traffic to ports within the same VLAN “community,” and channel traffic passing outside the community through promiscuous ports that have been mapped to the associated “primary” VLAN.
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 <i>switch-port mode</i> on page 256.)
<b>Example</b>:
Console(config)#vlan database
Console(config-vlan)#private-vlan 2 primary
Console(config-vlan)#private-vlan 3 community
Console(config)#</td></tr>
<tr><td><b>private vlan association</b>
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.</td><td><b>Syntax</b>:
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: 1-4094, no leading zeroes).
• secondary-vlan-id - ID of secondary (i.e, community) VLAN. (Range: 1-4094, no leading zeroes).
<b>Default Setting</b>: None
<b>Command Mode</b>: VLAN Configuration
<b>Command Usage</b>: 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).
<b>Example</b>:
Console(config-vlan)#private-vlan 2 association 3
Console(config)#</td></tr>
</table>

Configure Private VLAN Interfaces

Configure Private VLAN Interfaces	
Command	**Function**

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 communicate with all other host ports assigned to the same secondary VLAN. All communications outside of this VLAN must pass through a promiscuous port in the associated primary 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: Promiscuous ports assigned to a primary VLAN can communicate with all other promiscuous ports in the same VLAN, as well as with all the ports in the associated secondary VLANs.
	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: 2-4094, 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 a promiscuous port.
	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)#`

Display Private VLAN Information

Display Private VLAN Information	
Command	**Function**

show vlan private-vlan
Use this command to show the private VLAN configuration settings on this switch.
	Syntax:
	`show vlan private-vlan [community │ isolated │ primary]`
	• community – Displays all community VLANs, along with their associated primary VLAN and assigned host interfaces.
	• isolated – Displays all isolated VLANs, along with their associate 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`
	`     0          8      isolated`
	`Console#`

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.

GVRP and Bridge Extension Commands	
Command	**Function**

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)#`

show bridge-ext
This command shows the configuration for bridge extension commands.
	Default Setting: None
	Command Mode: Privileged Exec
	Command Usage: See *Enabling or Disabling GVRP (Global Setting)* on page 125 and *Displaying Bridge Extension Capabilities - Web* on page 28 for a description of the displayed items.
	Example:
	`Console#show bridge-ext`
	` Max support vlan numbers:                255`
	` Max support 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:                     Enabled`
	` GMRP:                                   Disabled`
	`Console#`

GVRP and Bridge Extension Commands (Cont.)

Command	**Function**

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 1/6`
	`Console(config-if)#switchport gvrp`
	`Console(config-if)#`

switchport forbidden vlan	See page 258.

show gvrp configuration
This command shows if GVRP is enabled.
	Syntax:
	`show gvrp configuration [interface]`
	• interface
	ethernet unit/port
	unit - Stack unit. (Range: 1-8)
	port - Port number. (Range: 1-26)
	port-channel channel-id (Range: 1-4)
	Default Setting: Shows both global and interface-specific configuration.
	Command Mode: Normal Exec, Privileged Exec
	Example:
	`Console#show gvrp configuration ethernet 1/6`
	`Eth 1/ 6:`
	` GVRP configuration: Enabled`
	`Console#`

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} - Which timer to set.`
	• timer_value - Value of timer.
	Ranges:
	• join: 20-1000 centiseconds
	• leave: 60-3000 centiseconds
	• leaveall: 500-18000 centiseconds
	Default Settings:
	• 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
	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)#`

GVRP and Bridge Extension Commands (Cont.)

Command	Function

show garp timer
This command shows the GARP timers for the selected interface.
	Syntax:
	`show garp timer [interface]`
	• interface
	ethernet unit/port
	unit - Stack unit. (Range: 1-8)
	port - Port number. (Range: 1-26)
	port-channel channel-id (Range: 1-4)
	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:      100 centiseconds`
	` Leave timer:     60 centiseconds`
	` Leaveall timer: 1000 centiseconds`
	`Console#`

Priority 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.

Priority Commands (Layer 2)

Configures default priority for untagged frames, sets queue weights, and maps class of service tags to hardware queues

Priority Commands (Layer 2)

Command	Function

queue mode
This command sets the queue 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.
	• wrr - Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights 1, 2, 4, 6 for queues 0 - 3 respectively.
	Default Setting: Weighted Round Robin
	Command Mode: Global Configuration
	Command Usage: You can set the switch to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before lower priority queues are serviced, or use Weighted Round-Robin (WRR) queuing that specifies a relative weight of each queue. WRR uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. 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)#`

show queue mode
This command shows the current queue mode.
	Default Setting: None
	Command Mode: Privileged Exec
	Example:
	`Console#show queue mode`
	
	`Queue mode: wrr`
	`Console#`

Priority Commands (Layer 2 - Cont.)

Command	**Function**

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 Port, IP Precedence or IP DSCP, and 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.
	This switch provides eight priority queues for each port. It is configured to use Weighted Round Robin, which can be viewed with the show queue bandwidth 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 0 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`

queue bandwidth
This command assigns weighted round-robin (WRR) weights to the four class of service (CoS) priority queues.
Use the no form to restore the default weights.
	Syntax:
	`queue bandwidth weight1...weight4`
	`no queue bandwidth`
	• weight1...weight4 - The ratio of weights for queues 0-3 determines the weights used by the WRR scheduler. However, note that Queue 0 is fixed at a weight of 1, and cannot be configured. (Range: 1-31)
	Default Setting: Weights 1, 2, 4, 6 are assigned to queues 0-3 respectively. Queue 0 is non-configurable.
	Command Mode: Global Configuration
	Command Usage: WRR controls bandwidth sharing at the egress port by defining scheduling weights.
	Example: This example shows how to assign WRR weights to priority queues 1 - 3:
	`Console(config)#queue bandwidth 6 9 12`
	`Console(config)#`

Priority Commands (Layer 2 - Cont.)

Command | **Function**

queue cos-map

This command assigns class of service (CoS) values to the priority queues (i.e., hardware output queues 0 - 3).

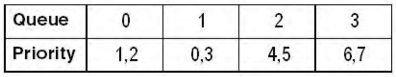
Use the no form set the CoS map to the default values.

Syntax:

```
queue cos-map queue_id [cos1 ... cosn]
no queue cos-map
```

- queue_id - The ID of the priority queue. Ranges are 0 to 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:



Queue	0	1	2	3
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 map CoS values 0, 1 and 2 to egress queue 0, value 3 to egress queue 1, values 4 and 5 to egress queue 2, and values 6 and 7 to egress queue 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue cos-map 0 0 1 2
Console(config-if)#queue cos-map 1 3
Console(config-if)#queue cos-map 2 4 5
Console(config-if)#queue cos-map 3 6 7
Console(config-if)#end
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 0 0 1 2 2 3 3
Console#
```

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        6
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: 1-8)

    port - Port number. (Range: 1-26)

  port-channel channel-id (Range: 1-4)

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: 0 0 0 1 2 2 3 3
Console#
```

Priority Commands (Layer 2 - Cont.)	
Command	**Function**
show interfaces switchport	See page 236.

Priority Commands (Layer 3 and 4)

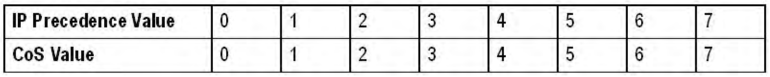
Maps TCP ports, IP precedence tags, or IP DSCP tags to class of service values

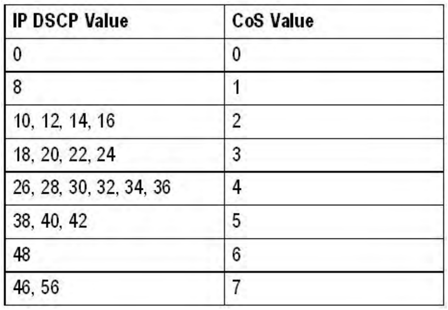
Priority Commands (Layer 3 and 4)	
Command	**Function**

map ip port (Global Configuration)
This command enables IP port mapping (i.e., class of service mapping for TCP/ UDP sockets).
Use the no form to disable IP port mapping.
	Syntax:
	`[no] map ip port`
	Default Setting: Disabled
	Command Mode: Global Configuration
	Command Usage: The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
	Example: The following example shows how to enable TCP/UDP port mapping globally:
	`Console(config)#map ip port`
	`Console(config)#`

map ip port (Interface Configuration)
This command set IP port priority (i.e., TCP/UDP port priority).
Use the no form to remove a specific setting.
	Syntax:
	`map ip port port number cos cos-value`
	`no map ip port port-number`
	• port-number - 16-bit TCP/UDP port number.(Range 1-65535)
	• cos-value - Class-of-Service value. (Range: 0-7)
	Default Setting: None
	Command Mode: Interface Configuration (Ethernet, Port Channel)
	Command Usage: The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
	This command sets the IP port priority for all interfaces.
	Example: The following example shows how to map HTTP traffic to CoS value 0:
	`Console(config)#interface ethernet 1/5`
	`Console(config-if)#map ip port 80 cos 0`
	`Console(config-if)#`

map ip precedence (Global Configuration)
This command enables IP precedence mapping (i.e., IP Type of Service).
Use the no form to disable IP precedence mapping.
	Syntax:
	`[no] map ip precedence`
	Default Setting: Disabled
	Command Mode: Global Configuration
	Command Usage: The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
	IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.
	Example: The following example shows how to enable IP precedence mapping globally:
	`Console(config)#map ip precedence`
	`Console(config)#`

<table>
<tr><th colspan="2">Priority Commands ((Layer 3 and 4)- Cont.)</th></tr>
<tr><th>Command</th><th>Function</th></tr>
<tr><td><b>map ip precedence
(Interface Configuration)</b>
This command sets IP precedence priority (i.e., IP Type of Service priority).
Use the no form to restore the default table.</td>
<td>Syntax:
<code>map ip precedence ip-precedence-value cos cos-value</code>
<code>no map ip precedence</code>
• precedence-value - 3-bit precedence value. (Range: 0-7)
• cos-value - Class-of-Service value (Range: 0-7)
Default Setting: The list below shows the default priority mapping
<i>Mapping IP Precedence Values</i>

<table><tr><td>IP Precedence Value</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr><tr><td>CoS Value</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr></table>
<b>Command Mode</b>: Interface Configuration (Ethernet, Port Channel)
<b>Command Usage</b>: The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
IP Precedence values are mapped to default Class of Service values on a one-to-one basis according to recommendations in the IEEE 802.1p standard, and then subsequently mapped to the eight hardware priority queues.
This command sets the IP Precedence for all interfaces.
<b>Example</b>: The following example shows how to map IP precedence value 1 to CoS value 0:
<code>Console(config)#interface ethernet 1/5</code>
<code>Console(config-if)#map ip precedence 1 cos 0</code>
<code>Console(config-if)#</code></td></tr>
<tr><td><b>map ip dscp
(Global Configuration)</b>
This command enables IP DSCP mapping (i.e., Differentiated Services Code Point mapping).
Use the no form to disable IP DSCP mapping.</td>
<td><b>Syntax</b>:
<code>[no] map ip dscp</code>
<b>Default Setting</b>: Disabled
<b>Command Mode</b>: Global Configuration
<b>Command Usage</b>: The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.
<b>Example</b>: The following example shows how to enable IP DSCP mapping globally:
<code>Console(config)#map ip dscp</code>
<code>Console(config)#</code></td></tr>
</table>

<table>
<tr><th colspan="2">Priority Commands ((Layer 3 and 4)- Cont.)</th></tr>
<tr><th>Command</th><th>Function</th></tr>
<tr><td><b>map ip dscp</b>
<b>(Interface Configuration)</b>
This command sets IP DSCP priority (i.e., Differentiated Services Code Point priority).
Use the no form to restore the default table.</td><td><b>Syntax</b>:<pre>
map ip dscp dscp-value cos cos-value
no map ip dscp
</pre>• dscp-value - 8-bit DSCP value. (Range: 0-63)
• cos-value - Class-of-Service value (Range: 0-7)
<b>Default Setting</b>: 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
<i>IP DSCP to CoS Values</i>
<table>
<tr><th>IP DSCP Value</th><th>CoS Value</th></tr>
<tr><td>0</td><td>0</td></tr>
<tr><td>8</td><td>1</td></tr>
<tr><td>10, 12, 14, 16</td><td>2</td></tr>
<tr><td>18, 20, 22, 24</td><td>3</td></tr>
<tr><td>26, 28, 30, 32, 34, 36</td><td>4</td></tr>
<tr><td>38, 40, 42</td><td>5</td></tr>
<tr><td>48</td><td>6</td></tr>
<tr><td>46, 56</td><td>7</td></tr>
</table><b>Command Mode</b>: Interface Configuration (Ethernet, Port Channel)
<b>Command Usage</b>: The precedence for priority mapping is IP Port, IP Precedence or 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.
<b>Example</b>: The following example shows how to map IP DSCP value 1 to CoS value 0:<pre>
Console(config)#interface ethernet 1/5
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#
</pre></td></tr>
<tr><td><b>show map ip port</b>
Use this command to show the IP port priority map.</td><td><b>Syntax</b>:<pre>
show map ip port [interface]
</pre>• interface
ethernet unit/port
unit - Stack unit. (Range: 1-8)
port - Port number. (Range: 1-26)
port-channel channel-id (Range: 1-4)
<b>Default Setting</b>: None
<b>Command Mode</b>: Privileged Exec
<b>Example</b>: The following shows that HTTP traffic has been mapped to CoS value 0:<pre>
Console#show map ip port
TCP port mapping status: disabled

 Port   Port no. COS
 --------- -------- ---
  Eth 1/ 5   80   0
Console#
</pre></td></tr>
<tr><td><b>map access-list ip</b></td><td>See page 216.</td></tr>
<tr><td><b>map access-list mac</b></td><td>See page 222.</td></tr>
</table>

Priority Commands ((Layer 3 and 4)- Cont.)

Command | **Function**

show map ip precedence

This command shows the IP precedence priority map.

Syntax:

```
show map ip precedence [interface]
```

- interface

  ethernet unit/port

  unit - Stack unit. (Range: 1-8)

  port - Port number. (Range: 1-26)

  port-channel channel-id (Range: 1-4)

Default Setting: None

Command Mode: Privileged Exec

Example:

```
Console#show map ip precedence ethernet 1/5
Precedence mapping status: disabled

 Port      Precedence COS
 --------- ---------- ---
  Eth 1/ 5          0   0
  Eth 1/ 5          1   1
  Eth 1/ 5          2   2
  Eth 1/ 5          3   3
  Eth 1/ 5          4   4
  Eth 1/ 5          5   5
  Eth 1/ 5          6   6
  Eth 1/ 5          7   7
Console#
```

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: 1-8)

  port - Port number. (Range: 1-26)

  port-channel channel-id (Range: 1-4)

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   0
  Eth 1/ 1   62   0
  Eth 1/ 1   63   0
Console#
```

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.

IGMP Snooping Commands

IGMP Snooping Commands	
Command	**Function**

ip igmp snooping
This command enables IGMP snooping on this 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 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 - Stack unit. (Range: 1-8)
	port - Port number. (Range: 1-26)
	port-channel channel-id (Range: 1-4)
	Default Setting: None
	Command Mode: Global Configuration
	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 version
This command configures the IGMP snooping version.
Use the no form to restore the default.
	Syntax:
	`ip igmp snooping version {1 | 2}`
	`no ip igmp snooping version`
	• 1 - IGMP Version 1
	• 2 - IGMP Version 2
	Default Setting: IGMP Version 2
	Command Mode: Global Configuration
	Command Usage: All systems on the subnet must support the same version. If there are legacy devices in your network that only support Version 1, you will also have to configure this switch to use Version 1.
	Some commands are only enabled for IGMPv2, including ip igmp query-max-response-time and ip igmp query-timeout.
	Example: The following configures the switch to use IGMP Version 1:
	`Console(config)#ip igmp snooping version 1`
	`Console(config)#`

IGMP Snooping Commands (Cont.)	
Command	**Function**

show ip igmp snooping
This command shows the IGMP snooping configuration.
	Default Setting: None
	Command Mode: Privileged Exec
	Command Usage: See “Configuring IGMP Snooping and Query Parameters” on page 3-137 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:           Enabled`
	` Query count:              2`
	` Query interval:           125 sec`
	` Query max response time:  10 sec`
	` Router port expire time:  300 sec`
	` IGMP snooping version:    Version 2`
	`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 to 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 (Layer 2)

IGMP Query Commands (Layer 2)	
Command	**Function**

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: 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)#`

IGMP Query Commands (Layer 2 - Cont.)

Command	**Function**

ip igmp snooping query-count
This command configures the query count.
Use the no form to restore the default.
	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)#`

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 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, 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)#`

IGMP Query Commands (Layer 2 - Cont.)	
Command	**Function**

ip igmp snooping router-port-expire-time
This command configures the query 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 the router port (i.e., the interface which had been receiving query packets) to have expired. (Range: 300-500)
	Default Setting: 300 seconds
	Command Mode: Global Configuration
	Command Usage: The switch must use IGMPv2 for this command to take effect.
	Example: The following shows how to configure the default timeout to 300 seconds:
	`Console(config)#ip igmp snooping router-port-expire-time`
	`300`
	`Console(config)#`

Static Multicast Routing Commands

Static Multicast Routing Commands	
Command	**Function**

ip igmp snooping vlan mrouter
This command statically configures a multicast router port.
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 - Stack unit. (Range: 1-8)
	port - Port number. (Range: 1-26)
	port-channel channel-id (Range: 1-4)
	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/switch connected over the network to an interface (port or trunk) on your router, you can manually configure that interface to join all the current multicast groups.
	Example: The following shows how to configure port 11 as a multicast router port within VLAN 1:
	`Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/`
	`11`
	`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 that port 11 in VLAN 1 is attached to a multicast router:
	`Console#show ip igmp snooping mrouter vlan 1`
	` VLAN M'cast Router Ports Type`
	` ---- ------------------- -------`
	`    1            Eth 1/11  Static`
	`    2            Eth 1/12  Static`
	`Console#`

IP Interface Commands

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. You may also need to a establish a default gateway between this device and the management stations.

IP Interface Commands

Command	**Function**

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} [secondary]`
	`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.
	• secondary - Specifies a secondary IP address.
	Default Setting: DHCP
	Command Mode: Interface Configuration (VLAN)
	Command Usage: If this router is directly connected to end node devices (or connected to end nodes via shared media) that will be assigned to a specific subnet, then you must create a router interface for each VLAN that will support routing. The router interface consists of an IP address and subnet mask. This interface address defines both the network number to which the router interface is attached and the router's host number on that network. In other words, a router interface address defines the network and subnetwork numbers of the segment that is connected to that interface, and allows you to send IP packets to or from the router.
	Before you configure any network interfaces on this router, you should first create a VLAN for each unique user group, or for each network application and its associated users. Then assign the ports associated with each of these VLANs.
	You must assign an IP address to this device to gain management access over the network. You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the configuration program.
	An interface can have only one primary IP address, but can have many secondary IP addresses. In other words, you will need to specify secondary addresses if more than one IP subnet can be accessed via this interface.
	If you select the bootp or dhcp option, IP is enabled but will not function until a BOOTP or DHCP reply has been received. Requests will be broadcast periodically by this device in an effort to learn its IP address. (BOOTP and DHCP values can include the IP address, default gateway, and subnet mask).
	You can start broadcasting BOOTP or DHCP requests by entering an ip dhcp restart command, or by rebooting the router switch.
	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.
	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)#`

IP Interface Commands (Cont.)

Command	Function

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 the static route.
	Syntax:
	`ip default-gateway gateway`
	`no ip default-gateway`
	• gateway - IP address of the default gateway
	Default Setting: No static route is established.
	Command Mode: Global Configuration
	Command Usage: 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)#`

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 via 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)#end`
	`Console#ip dhcp restart`
	`Console#show ip interface`
	` IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,`
	` and address mode: DHCP.`
	`Console#`

show ip interface
This command displays the settings of an IP interface.
	Default Setting: All interfaces
	Command Mode: Privileged Exec
	Example:
	`Console#show ip interface`
	` IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,`
	` and address mode:       User specified.`
	`Console#`

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#`

IP Interface Commands (Cont.)	
Command	**Function**

ping
This command sends ICMP echo request packets to another node on the network.
	Syntax:
	`ping host [size size] [count count]`
	• host - IP address or IP alias of the host.
	• size - Number of bytes in a packet. (Range: 32-512, default: 32) The actual packet size will be eight bytes larger than the size specified because the switch adds header information.
	• count - Number of packets to send. (Range: 1-16, default: 5)
	Default Setting: This command has no default for the host.
	Command Mode: Normal Exec, Privileged Exec
	Command Usage: Use the ping command to see if another site on the network can be reached.
	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.
	Press <Esc> to stop pinging.
	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: 10 ms`
	`Ping statistics for 10.1.0.9:`
	` 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)`
	`Approximate round trip times:`
	` Minimum = 10 ms, Maximum = 20 ms, Average = 10 ms`
	`Console#`

DNS Commands

These commands are used to configure Domain Naming System (DNS) services. You can manually configure entries in the DNS domain name to IP address mapping table, configure default domain names, or specify one or more name servers 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 (page 279) and domain lookup is enabled with the **ip domain-lookup** command (page 280).

DNS Commands

Command	Function

ip host
This command creates a static entry in the DNS table that maps a host name to an IP address.
Use the no form to remove an entry.
	Syntax:
	`[no] ip host name address1 [address2 … address8]`
	• name - Name of the host. (Range: 1-64 characters)
	• address1 - Corresponding IP address.
	• address2 … address8 - Additional corresponding IP addresses.
	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.
	Example: This example maps two 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`
	` 10.1.0.55 192.168.1.55`
	`Alias`
	`Console#`

clear host
This command deletes 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
	Example: This example clears all static entries from the DNS table:
	`Console(config)#clear host *`
	`Console(config)#`

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: 1-64 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#`

DNS Commands (Cont.)

Command	Function

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 server 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#`

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 domain-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#`

DNS Commands (Cont.)

<table>
<tr><th>Command</th><th>Function</th></tr>
<tr><td><b>ip domain-lookup</b>
This command enables DNS host name-to-address translation.
Use the no form to disable DNS.</td><td><b>Syntax</b>:<pre>[no] ip domain-lookup</pre><b>Default Setting</b>: Disabled
<b>Command Mode</b>: Global Configuration
<b>Command Usage</b>: At least one name server must be specified before you can enable DNS. If all name servers are deleted, DNS will automatically be disabled.
<b>Example</b>: This example enables DNS and then displays the configuration:<pre>
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#
</pre></td></tr>
<tr><td><b>show hosts</b>
This command displays the static host name-to-address mapping table.</td><td><b>Command Mode</b>: Privileged Exec
<b>Example</b>: 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:<pre>
Console#show hosts

Hostname
 rd5
Inet address
 10.1.0.55 192.168.1.55
Alias
 1.rd6
Console#
</pre></td></tr>
<tr><td><b>show dns</b>
This command displays the configuration of the DNS server.</td><td><b>Command Mode</b>: Privileged Exec
<b>Example</b>:<pre>
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#
</pre></td></tr>
</table>

<table>
<tr><th colspan="2">DNS Commands (Cont.)</th></tr>
<tr><th>Command</th><th>Function</th></tr>
<tr><td>

show dns cache

This command displays entries in the DNS cache.

</td><td>

Command Mode: Privileged Exec

Example:

```
Console#show dns cache
NO       FLAG     TYPE     IP               TTL      DOMAIN
0         4      CNAME   10.2.44.96       893     pttch_pc.accton.com.tw
1         4       CNAME   10.2.44.3        898      ahten.accton.com.tw
2         4       CNAME   66.218.71.84     298      www.yahoo.akadns.net
3         4       CNAME   66.218.71.83     298      www.yahoo.akadns.net
4         4       CNAME   66.218.71.81     298      www.yahoo.akadns.net
5         4       CNAME   66.218.71.80     298      www.yahoo.akadns.net
6         4       CNAME   66.218.71.89     298      www.yahoo.akadns.net
7         4       CNAME   66.218.71.86     298      www.yahoo.akadns.net
8         4       ALIAS   POINTER TO:7     298      www.yahoo.com
Console#
```

- 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 canonical or primary name for the owner, and ALIAS which specifies multiple domain names 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.

</td></tr>
<tr><td>

clear dns cache

This command clears all entries in the DNS cache.

</td><td>

Command Mode: Privileged Exec

Example:

```
Console#clear dns cache
Console#show dns cache
NO       FLAG     TYPE     IP               TTL      DOMAIN
Console#
```

</td></tr>
</table>

Troubleshooting

Troubleshooting Chart	
Symptom	**Action**
Cannot connect using Telnet, Web browser, or SNMP software	• Be sure you have configured the agent with a valid IP address, subnet mask and default gateway. • If you are trying to connect to the agent via the IP address for a tagged VLAN group, your management station must include the appropriate tag in its transmitted frames. • Check that you have a valid network connection to the switch and that the port you are using has not been disabled. • Check network cabling between the management station and the switch. • If you cannot connect using Telnet or SSH, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time.
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 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.

It's Your World - Take Control™

3000 RESEARCH DRIVE, RICHARDSON, TX 75082 USA • 800.222.0193 • 469.624.8000 • 469-624-7153 fax • 800.932.6993 technical support • www.amx.com