Sixnet® Series

# Gigabit Ethernet Switches

## MIL312 - MIL314 - MIL316 - MIL318

Software Manual | April 2015

## CONTACT INFORMATION :


## AMERICAS

York, PA: +1 (717) 767-6511
Mobile, AL: +1 (251) 342-2164
Ballston Lake, NY: +1 (518) 877-5173
**Hours:** 8am-6pm Eastern Standard Time
(UTC/GMT -5 hours)

## ASIA-PACIFIC

Shanghai, P.R. China: +86 21-6113-3688 x767
**Hours:** 10am-6pm China Standard Time
(UTC/GMT +8 hours)

## EUROPE

The Netherlands: +31 33-4723-225
**Hours:** 9am-6pm Central European Time
(UTC/GMT +1 hour)

Website: www.redlion.net

Email: customer.service@redlion.net

# ABOUT THIS MANUAL

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

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

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

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

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

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

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

The *Installation Guide*

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

**Revision History** The following information lists the release history of this document.

| Issue / Revision Date | Content Description |
|---|---|
| April 2015 | This manual is valid for software release v1.2.2.16.<br>Added VRRP (Virtual Router Redundancy Protocol) support for accept mode (RFC 5798).<br>Removed invalid references to stacking. |

# CONTENTS

# FIGURES

# TABLES

# GETTING STARTED

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

This section includes these chapters:

# 1 INTRODUCTION

This switch provides a broad range of features for Layer 2 switching and Layer 3 routing. It includes a management agent that allows you to configure the features listed in this manual. The default configuration can be used for most of the features provided by this switch. However, there are many options that you should configure to maximize the switch's performance for your particular network environment.

## KEY FEATURES

**Table 1: Key Features**

| Feature | Description |
|---|---|
| Configuration Backup and Restore | Using management station or FTP/TFTP server |
| Authentication | Console, Telnet, web – user name/password, RADIUS, TACACS+<br>Port – IEEE 802.1X, MAC address filtering<br>SNMP v1/2c - Community strings<br>SNMP version 3 – MD5 or SHA password<br>Telnet – SSH<br>Web – HTTPS |
| General Security Measures | AAA<br>ARP inspection<br>DHCP Snooping (with Option 82 relay information)<br>IP Source Guard<br>Private VLANs<br>Port Authentication – IEEE 802.1X<br>Port Security – MAC address filtering |
| Access Control Lists | Supports up to 256 ACLs, 96 MAC rules, 96 IP rules, and 96 IPv6 rules |
| DHCP | Client, Relay, Server |
| DNS | Client and Proxy service |
| Port Configuration | Speed and duplex mode and flow control |
| Port Trunking | Supports up to 25 trunks per switch – static or dynamic trunking (LACP) |
| Port Mirroring | 26 sessions, across switch, one or more source ports to one analysis port |
| Congestion Control | Rate Limiting<br>Throttling for broadcast storms |
| Address Table | Up to 16K MAC addresses in the forwarding table, 1024 static MAC addresses;<br>Up to 8K IPv4 and 4K IPv6 entries in the host table;<br>8K entries in the ARP cache, 256 static ARP entries;<br>8K IPv4 and 4K IPv6 entries in the IP routing table, 512 static IP routes, 512 IP interfaces;<br>1024 L2 multicast groups |
| IP Version 4 and 6 | Supports IPv4 and IPv6 addressing, and management |
| IEEE 802.1D Bridge | Supports dynamic data switching and addresses learning |

**Table 1: Key Features (Continued)**

| Feature | Description |
|---|---|
| Store-and-Forward Switching | Supported to ensure wire-speed switching while eliminating bad frames |
| Spanning Tree Algorithm | Supports standard STP, Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Trees (MSTP) |
| Virtual LANs | Up to 256 using IEEE 802.1Q, port-based, protocol-based, private VLANs, voice VLANs, and QinQ tunnel |
| Traffic Prioritization | Default port priority, traffic class map, queue scheduling, IP Precedence, or Differentiated Services Code Point (DSCP), and TCP/UDP Port |
| Qualify of Service | Supports Differentiated Services (DiffServ) |
| Link Layer Discovery Protocol | Used to discover basic information about neighboring devices |
| Router Redundancy | Router backup is provided with the Virtual Router Redundancy Protocol (VRRP) |
| IP Routing | Routing Information Protocol (RIP), Open Shortest Path First (OSPFv2/v3), static routes, Equal-Cost Multipath Routing (ECMP) |
| ARP | Static and dynamic address configuration, proxy ARP |
| Multicast Filtering | Supports IGMP snooping and query for Layer 2, IGMP for Layer 3, and Multicast VLAN Registration |
| Multicast Routing | Supports PIM-DM and PIM-SM for IPv4 and PIM-SM for IPv6 |

## 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. Untagged (port-based), tagged, and protocol-based VLANs, plus support for automatic GVRP VLAN registration provide traffic security and efficient use of network bandwidth. CoS priority queuing 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 the management station (using the web interface) or an FTP/TFTP server (using the web or console interface), and later download this file to restore the switch configuration settings.

### Authentication

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

Other authentication options include HTTPS for secure management access via the web, SSH for secure management access over a Telnet-equivalent connection, SNMP Version 3, IP address filtering for SNMP/Telnet/web management access. MAC address filtering and IP source guard also provide authenticated port access. While DHCP snooping is provided to prevent malicious attacks from insecure ports.

**Access Control Lists** ACLs provide packet filtering for 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** A DHCP server is provided to assign IP addresses to host devices. 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 full-duplex mode on ports whenever possible to double the throughput of switch connections. Flow control should also be enabled to control network traffic during periods of congestion and prevent the loss of packets when port buffer thresholds are exceeded. The switch supports flow control based on the IEEE 802.3x standard (now incorporated in IEEE 802.3-2002).

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

**Port Mirroring** The switch can unobtrusively mirror traffic from any port to a monitor port. You can then attach a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity.

**Port Trunking** Ports can be combined into an aggregate connection. Trunks can be manually set up or dynamically configured using Link Aggregation Control Protocol (LACP – IEEE 802.3-2005). The additional ports dramatically increase the throughput across any connection, and provide redundancy by taking over the load if a port in the trunk should fail. The switch supports up to 9 trunks depending on the model.

**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.

### IP Address Filtering

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

### IEEE 802.1D Bridge

The switch supports IEEE 802.1D transparent bridging. The address table facilitates data switching by learning addresses, and then filtering or forwarding traffic based on this information. The address table supports up to 16K 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 2 MB for frame buffering. This buffer can queue packets awaiting transmission on congested networks.

### Spanning Tree Algorithm

The switch supports these spanning tree protocols:

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

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

- Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s) – This protocol is a direct extension of RSTP. It can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group (as sometimes occurs with IEEE 802.1D STP).

**Virtual LANs** The switch supports up to 4093 VLANs. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. The switch supports tagged VLANs based on the IEEE 802.1Q standard. Members of VLAN groups can be dynamically learned via GVRP, or ports can be manually assigned to a specific set of VLANs. This allows the switch to restrict traffic to the VLAN groups to which a user has been assigned. By segmenting your network into VLANs, you can:

- Eliminate broadcast storms which severely degrade performance in a flat network.
- Simplify network management for node changes/moves by remotely configuring VLAN membership for any port, rather than having to manually change the network connection.
- Provide data security by restricting all traffic to the originating VLAN, 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.
- Use protocol VLANs to restrict traffic to specified interfaces based on protocol type.

**IEEE 802.1Q Tunneling (QinQ)** This feature is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting Service Provider VLAN (SPVLAN) tags into the customer’s frames when they enter the service provider’s network, and then stripping the tags when the frames leave the network.

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

This switch also supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic can be prioritized based on the priority bits in the IP frame’s Type of Service (ToS) octet using DSCP, IP Precedence, or TCP/UDP port numbers. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

**Quality of Service** Differentiated Services (DiffServ) provides policy-based management mechanisms used for prioritizing network resources to meet the requirements of specific traffic types on a per-hop basis. Each packet is classified upon entry into the network based on access lists, IP Precedence or DSCP values, or VLAN lists. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding.

### 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 static routing, Routing Information Protocol (RIP), Open Shortest Path First (OSPF) protocol.

Static Routing – Traffic is automatically routed between any IP interfaces configured on the MIL300-switch. Routing to statically configured hosts or subnet addresses is provided based on next-hop entries specified in the static routing table.

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. OSPFv2 is provided for routing IPv4 traffic, and OSPFv3 for routing IPv6 traffic.

### Equal-cost Multipath Load Balancing

When multiple paths to the same destination and with the same path cost are found in the routing table, the Equal-cost Multipath (ECMP) algorithm first checks if the cost is lower than that of any other routing entries. If the cost is the lowest in the table, the switch will use up to eight paths having the lowest path cost to balance traffic forwarded to the destination. ECMP uses either equal-cost unicast multipaths manually configured in the static routing table, or equal-cost multipaths dynamically detected by the Open Shortest Path Algorithm (OSPF). In other words, it uses either static or OSPF entries, not both.

### Router Redundancy

The Virtual Router Redundancy Protocol (VRRP) uses a virtual IP address to support a primary router and multiple backup routers. The backups can be configured to take over the workload if the master fails or to load share the traffic. The primary goal of this protocol is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

### Address Resolution Protocol

The switch uses ARP and Proxy ARP to convert between IP addresses and MAC (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. Either static or dynamic entries can be configured 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. It also supports Multicast VLAN Registration (MVR) which allows common multicast traffic, such as television channels, to be transmitted across a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, while preserving security and data isolation for normal traffic.

### Multicast Routing

Routing for multicast packets is supported by the Protocol-Independent Multicasting - Dense Mode and Sparse Mode (PIM-DM, PIM-SM) protocols. These protocols work in conjunction with IGMP to filter and route multicast traffic. 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. PIM-DM and PIM-SM are supported for IPv4 and PIM-SM for IPv6.

## SYSTEM DEFAULTS

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

The following table lists some of the basic system defaults.

**Table 2: System Defaults**

| Function | Parameter | Default |
|---|---|---|
| Console Port Connection | Baud Rate | 115200 bps |
| | Data bits | 8 |
| | Stop bits | 1 |
| | Parity | none |
| | Local Console Timeout | 0 (disabled) |

**Table 2: System Defaults (Continued)**

| Function | Parameter | Default |
|---|---|---|
| Authentication and Security Measures | Privileged Exec Level | Username “admin”<br>Password “admin” |
| | Normal Exec Level | Username “guest”<br>Password “guest” |
| | Enable Privileged Exec from Normal Exec Level | Password “super” |
| | RADIUS Authentication | Disabled |
| | TACACS+ Authentication | Disabled |
| | 802.1X Port Authentication | Disabled |
| | MAC Authentication | Disabled |
| | HTTPS | Enabled |
| | SSH | Disabled |
| | Port Security | Disabled |
| | IP Filtering | Disabled |
| | DHCP Snooping | Disabled |
| Web Management | HTTP Server | Enabled |
| | HTTP Port Number | 80 |
| | HTTP Secure Server | Disabled |
| | HTTP Secure Server Redirect | Disabled |
| SNMP | SNMP Agent | Enabled |
| | Community Strings | “public” (read only)<br>“private” (read/write) |
| | Traps | Authentication traps: enabled<br>Link-up-down events: enabled |
| | SNMP V3 | View: defaultview<br>Group: public (read only); private (read/write) |
| Port Configuration | Admin Status | Enabled |
| | Auto-negotiation | Enabled |
| | Flow Control | Disabled |
| Port Trunking | Static Trunks | None |
| | LACP (all ports) | Disabled |
| Congestion Control | Rate Limiting | Disabled |
| | Storm Control | Broadcast: Enabled<br>(500 packets/sec) |
| Address Table | Aging Time | 300 seconds |
| Spanning Tree Algorithm | Status | Enabled, RSTP<br>(Defaults: RSTP standard) |
| | Edge Ports | Enabled |
| LLDP | Status | Enabled |

**Table 2: System Defaults (Continued)**

| Function | Parameter | Default |
|---|---|---|
| Virtual LANs | Default VLAN | 1 |
| | PVID | 1 |
| | Acceptable Frame Type | All |
| | Ingress Filtering | Disabled |
| | Switchport Mode (Egress Mode) | Hybrid: tagged/untagged frames |
| | GVRP (global) | Disabled |
| | GVRP (port interface) | Disabled |
| | QinQ Tunneling | Disabled |
| Traffic Prioritization | Ingress Port Priority | 0 |
| | Queue Mode | WRR |
| | Weighted Round Robin | Queue: 0 1 2 3 4 5 6 7<br>Weight: 1 2 4 6 8 10 12 14 |
| | Class of Service | Enabled |
| | IP Precedence Priority | Disabled |
| | IP DSCP Priority | Disabled |
| | IP Port Priority | Disabled |
| IP Settings | Management. VLAN | Any VLAN configured with an IP address |
| | IP Address | DHCP assigned |
| | Default Gateway | 0.0.0.0 |
| | DHCP | Client: Enabled<br>Relay: Disabled<br>Server: Disabled |
| | DNS | Client/Proxy service: Disabled |
| | BOOTP | Disabled |
| | ARP | Enabled<br>Cache Timeout: 20 minutes<br>Proxy: Disabled |
| Unicast Routing | RIP | Disabled |
| | OSPFv2 | Disabled |
| | OSPFv3 | Disabled |
| Router Redundancy | VRRP | Disabled |
| Multicast Filtering | IGMP Snooping (Layer 2) | Snooping: Enabled<br>Querier: Disabled |
| | Multicast VLAN Registration | Disabled |
| | IGMP (Layer 3)<br>IGMP Proxy (Layer 3) | Disabled<br>Disabled |
| System Log | Status | Enabled |
| | Messages Logged | Levels 0-7 (all) |
| | Messages Logged to Flash | Levels 0-3 |

**Table 2: System Defaults (Continued)**

| Function | Parameter | Default |
|---|---|---|
| SMTP Email Alerts | Event Handler | Enabled (but no server defined) |
| SNTP | Clock Synchronization | Disabled |

# 2 INITIAL SWITCH CONFIGURATION

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

## CONNECTING TO THE SWITCH

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

**NOTE:** An IPv4 address for this switch is obtained via DHCP by default. To change this address, see "Setting an IP Address" on page 52.

### Configuration Options

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

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

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

The switch's web interface, console interface, and SNMP agent allow you to perform the following management functions:

- Set user names and passwords
- Set an IP interface for any VLAN
- Configure SNMP parameters
- Enable/disable any port
- Set the speed/duplex mode for any port
- Configure the bandwidth of any port by limiting input or output rates

- Control port access through IEEE 802.1X security or static address filtering
- Filter packets using Access Control Lists (ACLs)
- Configure up to 4093 IEEE 802.1Q VLANs
- Enable GVRP automatic VLAN registration
- Configure IP routing for unicast or multicast traffic
- Configure router redundancy
- Configure IGMP multicast filtering
- Upload and download system firmware or configuration files via HTTP (using the web interface) or FTP/TFTP (using the command line or web interface)
- Configure Spanning Tree parameters
- Configure Class of Service (CoS) priority queuing
- Configure static or LACP trunks
- Enable port mirroring
- Set storm control on any port for excessive broadcast traffic
- Display system information and statistics

## Required Connections

The switch provides an RS-232 serial port that enables a connection to a PC or terminal for monitoring and configuring the switch.

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

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

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.

Connect the other end of the cable to the RS-232 serial port on the switch.

Make sure the terminal emulation software is set as follows:

- Select the appropriate serial port (COM port 1 or COM port 2).
- Set the baud rate to 115200 bps.
- Set the data format to 8 data bits, 1 stop bit, and no parity.

- Set flow control to none.
- Set the emulation mode to VT100.
- When using HyperTerminal, select Terminal keys, not Windows keys.

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

For a description of how to use the CLI, see "Using the Command Line Interface" on page 599. For a list of all the CLI commands and detailed information on using the CLI, refer to "CLI Command Groups" on page 608.

### Remote Connections

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

An IPv4 address for this switch is obtained via DHCP by default. To manually configure this address or enable dynamic address assignment via DHCP, see "Setting an IP Address" on page 52.

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

**NOTE:** Any VLAN group can be assigned an IP interface address (page 52) for managing the switch. Also, note that the Master unit does not have to include an active port member in the VLAN interface used for management access.

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, Netscape 6.2 or above, or Mozilla Firefox 2.0.0.0 or above), or from a network computer using SNMP network management software.

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

## BASIC CONFIGURATION

### Console Connection

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

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

To initiate your console connection, press <Enter>. The “User Access Verification” procedure starts.

At the Username prompt, enter “admin.”

At the Password prompt, also enter “admin.” (The password characters are not displayed on the console screen.)

The session is opened and the CLI displays the “Console#” prompt indicating you have access at the Privileged Exec level.

## Setting Passwords

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

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

Open the console interface with the default user name and password “admin” to access the Privileged Exec level.

Type “configure” and press <Enter>.

Type “username guest password 0 *password*,” for the Normal Exec level, where *password* is your new password. Press <Enter>.

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 EL 326 is opened.
 To end the CLI session, enter [Exit].

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

* This manual is based on the EL326 switch. Other than the difference in the number of ports, there are no significant differences. Therefore nearly all of the screen display examples are based on the EL326.

## Setting an IP Address

The switch can be configured manually for a static IP address or dynamically to obtain an IP address via BOOTP or DHCP

- **Manual** — You have to input the information, including IP address and subnet mask.
- **Dynamic** — The switch can send IPv4 configuration requests to BOOTP or DHCP address allocation servers on the network. An IPv6 link local address for use in a local network can be dynamically generated as described in "Obtaining an IPv6 Address" on page 57.

  The current software does not support DHCP for IPv6, so an IPv6 global unicast address for use in a network containing more than one subnet can only be manually configured as described in "Assigning an IPv6 Address" on page 54.

## 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 IPv4 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 default IPv4 address for this switch is 192.168.0.1 255.255.255.0.

### ASSIGNING AN IPV4 ADDRESS

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

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

To assign an IPv4 address to the switch, complete the following steps

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

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>.

Type “exit” to return to the global configuration mode prompt. Press <Enter>.

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
```

### ASSIGNING AN IPV6 ADDRESS

This section describes how to configure a “link local” address for connectivity within the local subnet only, and also how to configure a “global unicast” address, including a network prefix for use on a multi-segment network and the host portion of the address.

An IPv6 prefix or address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used to indicate the appropriate number of zeros required to fill the undefined fields. For detailed information on the other ways to assign IPv6 addresses, see "Setting the Switch’s IP Address (IP Version 6)" on page 420.

Link Local Address — All link-local addresses must be configured with a prefix of FE80. Remember that this address type makes the switch accessible over IPv6 for all devices attached to the same local subnet only. Also, if the switch detects that the address you configured conflicts with that in use by another device on the subnet, it will stop using the address in question, and automatically generate a link local address that does not conflict with any other devices on the local subnet.

To configure an IPv6 link local address for the switch, complete the following steps:

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

Type “ipv6 address” followed by up to 8 colon-separated 16-bit hexadecimal values for the *ipv6-address* similar to that shown in the example, followed by the “link-local” command parameter. Then press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address FE80::260:3EFF:FE11:6700 link-local
Console(config-if)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::260:3EFF:FE11:6700/64
Global unicast address(es):
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF11:6700/104
MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
Console#
```

Address for Multi-segment Network — Before you can assign an IPv6 address to the switch that will be used to connect to a multi-segment network, you must obtain the following information from your network administrator:

- Prefix for this network
- IP address for the switch
- Default gateway for the network

For networks that encompass several different subnets, you must define the full address, including a network prefix and the host address for the switch. You can specify either the full IPv6 address, or the IPv6 address and prefix length. The prefix length for an IPv6 network is the number of bits (from the left) of the prefix that form the network address, and is expressed as a decimal number. For example, all IPv6 addresses that start with the first byte of 73 (hexadecimal) could be expressed as 73:0:0:0:0:0:0:0/8 or 73::/8.

To generate an IPv6 global unicast address for the switch, complete the following steps:

From the global configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.

From the interface prompt, type “ipv6 address *ipv6-address*” or “ipv6 address *ipv6-address/prefix-length*,” where “prefix-length” indicates the address bits used to form the network portion of the address. (The network address starts from the left of the prefix and should encompass some of the ipv6-address bits.) The remaining bits are assigned to the host interface. Press <Enter>.

Type “exit” to return to the global configuration mode prompt. Press <Enter>.

To set the IP address of the IPv6 default gateway for the network to which the switch belongs, type “ipv6 default-gateway *gateway*,” where “gateway” is the IPv6 address of the default gateway. Press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2001:DB8:2222:7272::/64
Console(config-if)#ipv6 enable
Console(config-if)#exit
Console(config)#ipv6 default-gateway 2001:DB8:2222:7272::254
Console(config)end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::200:E8FF:FE93:82A0/64
Global unicast address(es):
  2001:DB8:2222:7272::/64, subnet is 2001:DB8:2222:7272::/64
  2005::212:CFFF:FE0B:4600, subnet is ::
Joined group address(es):
FF02::1:2
FF02::1:FF00:0
FF02::1:FF93:82A0
FF02::1
IPv6 link MTU is 1280 bytes
ND DAD is enabled, number of DAD attempts: 2.
ND retransmit interval is 1000 milliseconds
Console#
```

## DYNAMIC CONFIGURATION

*Obtaining an IPv4 Address*

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

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

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

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

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

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

- To obtain IP settings via DHCP, type “ip address dhcp” and press <Enter>.
- To obtain IP settings via BOOTP, type “ip address bootp” and press <Enter>.

Type “end” to return to the Privileged Exec mode. Press <Enter>.

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

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

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

\Write to FLASH finish.
Success.
```

### OBTAINING AN IPV6 ADDRESS

Link Local Address — There are several ways to configure IPv6 addresses. The simplest method is to automatically generate a “link local” address (identified by an address prefix of FE80). This address type makes the switch accessible over IPv6 for all devices attached to the same local subnet.

To generate an IPv6 link local address for the switch, complete the following steps:

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

Type “ipv6 enable” and press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 enable
Console(config-if)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::200:E8FF:FE90:0/64
Global unicast address(es):
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF90:0/104
MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
Console#
```

Address for Multi-segment Network — An IPv6 address for use in a network containing more than one subnet must be manually configured as described in "Assigning an IPv6 Address" on page 54. The current software does not support DHCP for IPv6.

## Enabling SNMP Management Access

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

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

The switch includes an SNMP agent that supports SNMP version 1, 2c, and 3 clients. To provide management access for version 1 or 2c clients, you must specify a community string. The switch provides a default MIB View (i.e., an SNMPv3 construct) for the default “public” community string that provides read access to the entire MIB tree, and a default view for the “private” community string that provides read/write access to the entire MIB tree. However, you may assign new views to version 1 or 2c community strings that suit your specific security requirements (see "Setting SNMPv3 Views" on page 348).

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

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

The default strings are:

- **public** - with read-only access. Authorized management stations are only able to retrieve MIB objects.

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

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

To configure a community string, complete the following steps:

From the Privileged Exec level global configuration mode prompt, type “snmp-server community *string mode*,” where “string” is the community access string and “mode” is **rw** (read/write) or **ro** (read only). Press <Enter>. (Note that the default mode is read only.)

To remove an existing string, simply type “no snmp-server community *string*,” where “string” is the community access string to remove. Press <Enter>.

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

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

### TRAP RECEIVERS

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

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

where “host-address” is the IP address for the trap receiver, “community-string” specifies access rights for a version 1/2c host, or is the user name of a version 3 host, “version” indicates the SNMP client version, and “auth | noauth | priv” means that authentication, no authentication, or authentication and privacy is used for v3 clients. Then press <Enter>. For a more detailed description of these parameters, see "snmp-server host" on page 664. The following example creates a trap host for each type of SNMP client.

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

### Configuring Access for SNMP Version 3 Clients

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

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

For a more detailed explanation on how to configure the switch for access from SNMP v3 clients, refer to "Simple Network Management Protocol" on page 343, or refer to the specific CLI commands for SNMP starting on page 659

## Managing System Files

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

The types of files are:

- **Configuration** — This file type stores system configuration information and is created when configuration settings are saved. Saved configuration files can be selected as a system start-up file or can be uploaded via FTP/TFTP to a server for backup. The file named “Factory_Default_Config.cfg” contains all the system default settings and cannot be deleted from the system. If the system is booted with the factory default settings, the master unit will also create a file named “startup1.cfg” that contains system settings information about the unit identifier, MAC address for each unit, and installed module types for each unit. The configuration settings from the factory defaults configuration file are copied to this file, which is then used to boot the switch. See "Saving or Restoring Configuration Settings" on page 60 for more information.

- **Operation Code** — System software that is executed after boot-up, also known as run-time code. This code runs the switch operations and provides the CLI and web management interfaces. See "Managing System Files" on page 90 for more information.

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

Due to the size limit of the flash memory, the switch supports only two operation code files. However, you can have as many diagnostic code files and configuration files as available flash memory space allows. The switch has a total of 32 Mbytes of flash memory for system files.

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

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

## Saving or Restoring Configuration Settings

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

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

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

The maximum number of saved configuration files depends on available flash memory. The amount of available flash memory can be checked by using the **dir** command.

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

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

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#
```

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

From the Privileged Exec mode prompt, type “copy tftp startup-config” and press <Enter>.

Enter the address of the TFTP server. Press <Enter>.

Enter the name of the startup file stored on the server. Press <Enter>.

Enter the name for the startup file on the switch. Press <Enter>.

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

Success.
Console#
```

# WEB CONFIGURATION

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

This section includes these chapters:

# 3 USING THE WEB INTERFACE

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

You can also use the Command Line Interface (CLI) to manage the switch over a serial connection to the console port or via Telnet. For more information on using the CLI, refer to "Using the Command Line Interface" on page 599."

## CONNECTING TO THE WEB INTERFACE

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

1. Configure the switch with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection, BOOTP or DHCP protocol. (See "Setting an IP Address" on page 52.)

2. Set user names and passwords using an out-of-band serial connection. Access to the web agent is controlled by the same user names and passwords as the onboard configuration program. (See "Setting Passwords" on page 52.)

3. After you enter a user name and password, you will have access to the system configuration program.

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 "Configuring Interface Settings for STA" on page 187.

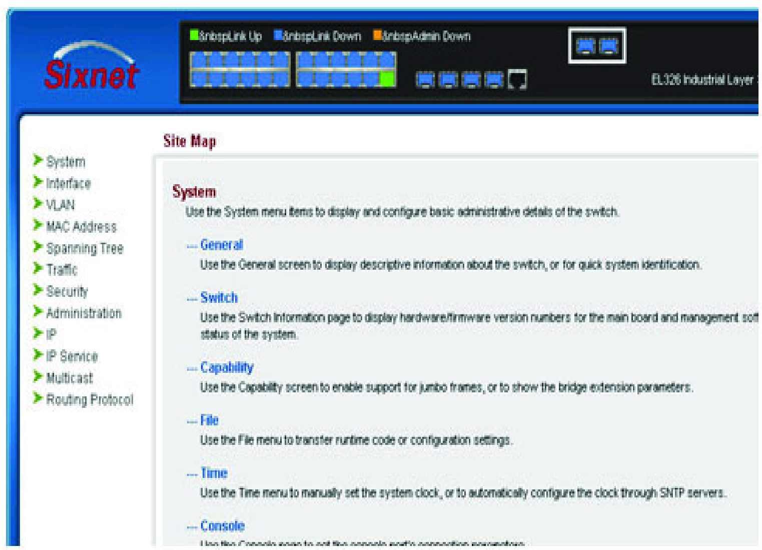
## NAVIGATING THE WEB BROWSER INTERFACE

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

### Home Page

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

**Figure 1: Home Page**




This manual is based on the EL 326 Gigabit Ethernet switch. Other than the number of ports supported by these models, there are no significant differences. Therefore nearly all of the screen display examples are based on the EL 326. The panel graphics for the switch types are shown on the following page.

You can open a connection to the manufacturer’s web site by clicking on the Sixnet® logo.

## Configuration Options

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

**Table 1: Web Page Configuration Buttons**

| Button | Action |
|---|---|
| Apply | Sets specified values to the system. |
| Revert | Cancels specified values and restores current values prior to pressing “Apply.” |
|  | Displays help for the selected page. |
|  | Refreshes the current page. |
|  | Displays the site map. |
|  | Logs out of the management interface. |
|  | Sends mail to the manufacturer. |
|  | Links to the manufacture’s web site. |

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

## Panel Display

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

**Figure 2: Front Panel Indicators**

## Main Menu

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

**Table 2: Switch Main Menu**

| Menu | Description | Page |
|---|---|---|
| System | | |
| General | Provides basic system description, including contact information | 85 |
| Switch | Shows the number of ports, hardware version, power status, and firmware version numbers | 86 |
| Capability | Enables support for jumbo frames; shows the bridge extension parameters | 88 |
| File | | 90 |
| Copy | Allows the transfer and copying files | 90 |
| Set Startup | Sets the startup file | 93 |
| Show | Shows the files stored in flash memory; allows deletion of files | 94 |
| Time | | 95 |
| Configure General | | |
| Manual | Manually sets the current time | 95 |
| SNTP | Configures SNTP polling interval | 96 |
| Configure Time Server | Configures a list of SNTP servers | 97 |
| Configure Time Zone | Sets the local time zone for the system clock | 98 |
| Console | Sets console port connection parameters | 98 |
| Telnet | Sets Telnet connection parameters | 100 |
| CPU Utilization | Displays information on CPU utilization | 102 |
| Memory Status | Shows memory utilization parameters | 102 |
| Reset | Restarts the switch immediately, at a specified time, after a specified delay, or at a periodic interval | 103 |
| Interface | | |
| Port | | |
| General | | |
| Configure by Port List | Configures connection settings per port | 107 |
| Configure by Port Range | Configures connection settings for a range of ports | 110 |
| Show Information | Displays port connection status | 110 |
| Mirror | | |
| Add | Sets the source and target ports for mirroring | 112 |
| Show | Shows the configured mirror sessions | 112 |
| Statistics | Shows Interface, Etherlike, RMON and Utilization port statistics | 113 |
| Chart | Shows Interface, Etherlike, RMON and Utilization port statistics | 113 |
| Cable Test | Performs cable diagnostics for selected port to diagnose any cable faults (short, open etc.) and report the cable length | 117 |

**Table 2: Switch Main Menu (Continued)**

| Menu | Description | Page |
|---|---|---|
| Trunk | | |
| Static | | |
| Configure Trunk | | |
| Add | Creates a trunk, along with the first port member | 119 |
| Show | Shows the configured trunk identifiers | 119 |
| Add Member | Specifies ports to group into static trunks | 119 |
| Show Member | Shows the port members for the selected trunk | 119 |
| Configure General | | |
| Configure | Configures trunk connection settings | 119 |
| Show Information | Displays trunk connection settings | 119 |
| Dynamic | | 122 |
| Configure Aggregator | Configures administration key for specific LACP groups | 122 |
| Configure Aggregation Port | | |
| Configure | | |
| General | Allows ports to dynamically join trunks | 122 |
| Actor | Configures parameters for link aggregation group members on the local side | 122 |
| Partner | Configures parameters for link aggregation group members on the remote side | 122 |
| Show Information | | |
| Counters | Displays statistics for LACP protocol messages | 127 |
| Internal | Displays configuration settings and operational state for the local side of a link aggregation | 128 |
| Neighbors | Displays configuration settings and operational state for the remote side of a link aggregation | 130 |
| Configure Trunk | | |
| Configure | Configures connection settings | 122 |
| Show | Displays port connection status | 122 |
| Show Member | Shows the active members in a trunk | 122 |
| Statistics | Shows Interface, Etherlike, RMON and Utilization trunk statistics | 113 |
| Chart | Shows Interface, Etherlike, RMON and Utilization trunk statistics | 113 |
| sFlow | Configures flow sampling for source and destination ports | 131 |
| Traffic Segmentation | | |
| Configure Global | Enables traffic segmentation globally | 133 |
| Configure Session | Configures the uplink and down-link ports for a segmented group of ports | 134 |
| VLAN Trunking | Allows unknown VLAN groups to pass through the specified interface | 135 |

**Table 2: Switch Main Menu (Continued)**

| Menu | Description | Page |
|---|---|---|
| VLAN | Virtual LAN | |
| Static | | |
| Add | Creates VLAN groups | 140 |
| Show | Displays configured VLAN groups | 140 |
| Modify | Configures group name and administrative status | 140 |
| Edit Member by VLAN | Specifies VLAN attributes per VLAN | 142 |
| Edit Member by Interface | Specifies VLAN attributes per interface | 142 |
| Edit Member by Interface Range | Specifies VLAN attributes per interface range | 142 |
| Dynamic | | |
| Configure General | Enables GVRP VLAN registration protocol globally | 147 |
| Configure Interface | Configures GVRP status and timers per interface | 147 |
| Show Dynamic VLAN | | |
| Show VLAN | Shows the VLANs this switch has joined through GVRP | 147 |
| Show VLAN Member | Shows the interfaces assigned to a VLAN through GVRP | 147 |
| Private | | |
| Configure VLAN | | |
| Add | Creates primary or community VLANs | 150 |
| Show | Display configured primary and community VLANs | 150 |
| Add Community VLAN | Associates a community VLAN with a primary VLAN | 152 |
| Show Community VLAN | Shows the community VLANs associated with a primary VLAN | 152 |
| Configure Interface | Sets the private VLAN interface type, and associates the interfaces with a private VLAN | 153 |
| Tunnel | IEEE 802.1Q (QinQ) Tunneling | 155 |
| Configure Global | Sets tunnel mode for the switch | 158 |
| Configure Interface | Sets the tunnel mode for any participating interface | 159 |
| Protocol | | |
| Configure Protocol | | |
| Add | Creates a protocol group, specifying supported protocols | 162 |
| Show | Shows configured protocol groups | 162 |
| Configure Interface | | |
| Add | Maps a protocol group to a VLAN | 163 |
| Show | Shows the protocol groups mapped to each VLAN | 163 |
| IP Subnet | | |
| Add | Maps IP subnet traffic to a VLAN | 165 |
| Show | Shows IP subnet to VLAN mapping | 165 |
| MAC-Based | | |
| Add | Maps traffic with specified source MAC address to a VLAN | 167 |

**Table 2: Switch Main Menu (Continued)**

| Menu | Description | Page |
|---|---|---|
| Show | Shows source MAC address to VLAN mapping | 167 |
| MAC Address | | |
| Learning Status | Enables MAC address learning on selected interfaces | 169 |
| Static | | |
| Add | Configures static entries in the address table | 170 |
| Show | Displays static entries in the address table | 170 |
| Dynamic | | |
| Configure Aging | Sets timeout for dynamically learned entries | 172 |
| Show Dynamic MAC | Displays dynamic entries in the address table | 173 |
| Clear Dynamic MAC | Removes any learned entries from the forwarding database and clears the transmit and receive counts for any static or system configured entries | 174 |
| Spanning Tree | | |
| Loopback Detection | Configures Loopback Detection parameters | 179 |
| STA | Spanning Tree Algorithm | |
| Configure Global | | |
| Configure | Configures global bridge settings for STP, RSTP and MSTP | 181 |
| Show Information | Displays STA values used for the bridge | 186 |
| Configure Interface | | |
| Configure | Configures interface settings for STA | 187 |
| Show Informaton | Displays interface settings for STA | 190 |
| MSTP | Multiple Spanning Tree Algorithm | |
| Configure Global | | |
| Add | Configures initial VLAN and priority for an MST instance | 193 |
| Show | Configures global settings for an MST instance | 193 |
| Modify | Modify priority for an MST instance | 193 |
| Add Member | Adds VLAN members for an MST instance | 193 |
| Show Member | Displays or deletes VLAN members for an MST instance | 193 |
| Show Information | Displays MSTP values used for the bridge | 193 |
| Configure Interface | | |
| Configure | Configures interface settings for an MST instance | 197 |
| Show Informaton | Displays interface settings for an MST instance | 197 |
| Traffic | | |
| Rate Limit | Sets the input and output rate limits for a port | 199 |
| Storm Control | Sets the broadcast storm threshold for each interface | 201 |
| Priority | | |
| Default Priority | Sets the default priority for each port or trunk | 203 |

**Table 2: Switch Main Menu (Continued)**

| Menu | Description | Page |
|---|---|---|
| Queue | Sets queue mode for the switch; sets the service weight for each queue that will use a weighted or hybrid mode | 204 |
| CoS to Queue | Specifies the hardware output queues to use for CoS priority tagged traffic | 207 |
| IP DSCP to CoS | Maps IP DSCP priorities found in ingress packets to CoS values for internal priority processing | 210 |
| IP Precedence to CoS | Maps IP Precedence priorities found in ingress packets to CoS values for internal priority processing | 213 |
| IP Port to CoS | Maps network applications designated by a TCP/UDP destination port number in the frame header to CoS values for internal processing | 215 |
| DiffServ | | |
| Configure Class | | |
| Add | Creates a class map for a type of traffic | 218 |
| Show | Shows configured class maps | 218 |
| Modify | Modifies the name of a class map | 218 |
| Add Rule | Configures the criteria used to classify ingress traffic | 218 |
| Show Rule | Shows the traffic classification rules for a class map | 218 |
| Configure Policy | | |
| Add | Creates a policy map to apply to multiple interfaces | 221 |
| Show | Shows configured policy maps | 221 |
| Modify | Modifies the name of a policy map | 221 |
| Add Rule | Sets the boundary parameters used for monitoring inbound traffic, and the action to take for conforming and non-conforming traffic | 221 |
| Show Rule | Shows the rules used to enforce bandwidth policing for a policy map | 221 |
| Configure Interface | Applies a policy map to an ingress port | 230 |
| VoIP | Voice over IP | 231 |
| Configure Global | Configures auto-detection of VoIP traffic, sets the Voice VLAN, and VLAN aging time | 231 |
| Configure OUI | | 232 |
| Add | Maps the OUI in the source MAC address of ingress packets to the VoIP device manufacturer | 232 |
| Show | Shows the OUI telephony list | 232 |
| Configure Interface | Configures VoIP traffic settings for ports, including the way in which a port is added to the Voice VLAN, filtering of non-VoIP packets, the method of detecting VoIP traffic, and the priority assigned to the voice traffic | 234 |
| Security | | 237 |
| AAA | Authentication, Authorization and Accounting | |
| System Authentication | Configures authentication sequence – local, RADIUS, and TACACS | 239 |
| Server | | 240 |
| Configure Server | Configures RADIUS and TACACS server message exchange settings | 240 |
| Configure Group | | |
| Add | Specifies a group of authentication servers and sets the priority sequence | 240 |

**Table 2: Switch Main Menu (Continued)**

| Menu | Description | Page |
|---|---|---|
| Show | Shows the authentication server groups and priority sequence | 240 |
| Accounting | Enables accounting of requested services for billing or security purposes | 244 |
| Configure Global | Specifies the interval at which the local accounting service updates information to the accounting server | 244 |
| Configure Method | | 244 |
| Add | Configures accounting for various service types | 244 |
| Show | Shows the accounting settings used for various service types | 244 |
| Configure Service | Sets the accounting method applied to specific interfaces for 802.1X, CLI command privilege levels for the console port, and for Telnet | 244 |
| Show Information | | 244 |
| Summary | Shows the configured accounting methods, and the methods applied to specific interfaces | 244 |
| Statistics | Shows basic accounting information recorded for user sessions | 244 |
| Authorization | Enables authorization of requested services | 249 |
| Configure Method | | 249 |
| Add | Configures authorization for various service types | 249 |
| Show | Shows the authorization settings used for various service types | 249 |
| Configure Service | Sets the authorization method applied used for the console port, and for Telnet | 249 |
| Show Information | Shows the configured authorization methods, and the methods applied to specific interfaces | 249 |
| User Accounts | | 252 |
| Add | Configures user names, passwords, and access levels | 252 |
| Show | Shows authorized users | 252 |
| Modify | Modifies user attributes | 252 |
| Web Authentication | Allows stations to authenticate and access the network in situations where 802.1X or MAC Authentication are infeasible or impractical | 253 |
| Configure Global | Enables web authentication globally, and sets message exchange parameters | 254 |
| Configure Interface | Enables web authentication on specified ports | 255 |
| Network Access | MAC address-based network access authentication | 256 |
| Configure Global | Enables aging for authenticated MAC addresses, and sets the time period after which a connected MAC address must be reauthenticated | 258 |
| Configure Interface | | 259 |
| General | Enables MAC authentication on a port; sets the maximum number of address that can be authenticated, the guest VLAN, dynamic VLAN and dynamic QoS | 259 |
| Link Detection | Configures detection of changes in link status, and the response (i.e., send trap or shut down port) | 261 |
| Configure MAC Filter | | 262 |
| Add | Specifies MAC addresses exempt from authentication | 262 |
| Show | Shows the list of exempt MAC addresses | 262 |

**Table 2: Switch Main Menu (Continued)**

| Menu | Description | Page |
|---|---|---|
| Show Information | Shows the authenticated MAC address list | 263 |
| HTTPS | Secure HTTP | 265 |
| Configure Global | Enables HTTPs, and specifies the UDP port to use | 265 |
| Copy Certificate | Replaces the default secure-site certificate | 266 |
| SSH | Secure Shell | 268 |
| Configure Global | Configures SSH server settings | 270 |
| Configure Host Key | | 272 |
| Generate | Generates the host key pair (public and private) | 272 |
| Show | Displays RSA and DSA host keys; deletes host keys | 272 |
| Configure User Key | | 273 |
| Copy | Imports user public keys from TFTP server | 273 |
| Show | Displays RSA and DSA user keys; deletes user keys | 273 |
| ACL | Access Control Lists | 275 |
| Configure Time Range | Configures the time to apply an ACL | 276 |
| Add | Specifies the name of a time range | 276 |
| Show | Shows the name of configured time ranges | 276 |
| Add Rule | | 276 |
| Absolute | Sets exact time or time range | 276 |
| Periodic | Sets a recurrent time | 276 |
| Show Rule | Shows the time specified by a rule | 276 |
| Configure ACL | | 280 |
| Show TCAM | Shows utilization parameters for TCAM | 279 |
| Add | Adds an ACL based on IP or MAC address filtering | 280 |
| Show | Shows the name and type of configured ACLs | 280 |
| Add Rule | Configures packet filtering based on IP or MAC addresses and other packet attributes | 280 |
| Show Rule | Shows the rules specified for an ACL | 280 |
| Configure Interface | Binds a port to the specified ACL and time range | 293 |
| ARP Inspection | | 294 |
| Configure General | Enables inspection globally, configures validation of additional address components, and sets the log rate for packet inspection | 295 |
| Configure VLAN | Enables ARP inspection on specified VLANs | 297 |
| Configure Interface | Sets the trust mode for ports, and sets the rate limit for packet inspection | 298 |
| Show Information | | |
| Show Statistics | Displays statistics on the inspection process | 300 |
| Show Log | Shows the inspection log list | 301 |
| IP Filter | | 302 |

**Table 2: Switch Main Menu (Continued)**

| Menu | Description | Page |
|---|---|---|
| Add | Sets IP addresses of clients allowed management access via the web, SNMP, and Telnet | 302 |
| Show | Shows the addresses to be allowed management access | 302 |
| Port Security | Configures per port security, including status, response for security breach, and maximum allowed MAC addresses | 304 |
| Port Authentication | IEEE 802.1X | 305 |
| Configure Global | Enables authentication and EAPOL pass-through | 307 |
| Configure Interface | Sets authentication parameters for individual ports | 308 |
| Show Statistics | Displays protocol statistics for the selected port | 312 |
| IP Source Guard | Filters IP traffic based on static entries in the IP Source Guard table, or dynamic entries in the DHCP Snooping table | 313 |
| Port Configuration | Enables IP source guard and selects filter type per port | 313 |
| Static Binding | | 315 |
| Add | Adds a static addresses to the source-guard binding table | 315 |
| Show | Shows static addresses in the source-guard binding table | 315 |
| Dynamic Binding | Displays the source-guard binding table for a selected interface | 317 |
| Administration | | 325 |
| Log | | 325 |
| System | | 325 |
| Configure Global | Stores error messages in local memory | 325 |
| Show System Logs | Shows logged error messages | 325 |
| Remote | Configures the logging of messages to a remote logging process | 328 |
| SMTP | Sends an SMTP client message to a participating server | 329 |
| LLDP | Link Layer Discovery Protocol | 330 |
| Configure Global | Configures global LLDP timing parameters | 330 |
| Configure Interface | Sets the message transmission mode; enables SNMP notification; and sets the LLDP attributes to advertise | 332 |
| Show Local Device Information | | 335 |
| General | Displays general information about the local device | 335 |
| Port/Trunk | Displays information about each interface | 335 |
| Show Remote Device Information | | 337 |
| Port/Trunk | Displays information about a remote device connected to a port on this switch | 337 |
| Port/Trunk Details | Displays detailed information about a remote device connected to this switch | 337 |
| Show Device Statistics | | 341 |
| General | Displays statistics for all connected remote devices | 341 |
| Port/Trunk | Displays statistics for remote devices on a selected port or trunk | 341 |
| SNMP | Simple Network Management Protocol | 343 |

**Table 2: Switch Main Menu (Continued)**

| Menu | Description | Page |
|---|---|---|
| Configure Global | Enables SNMP agent status, and sets related trap functions | 345 |
| Configure Engine | | |
| Set Engine ID | Sets the SNMP v3 engine ID on this switch | 346 |
| Add Remote Engine | Sets the SNMP v3 engine ID for a remote device | 347 |
| Show Remote Engine | Shows configured engine ID for remote devices | 347 |
| Configure View | | 348 |
| Add View | Adds an SNMP v3 view of the OID MIB | 348 |
| Show View | Shows configured SNMP v3 views | 348 |
| Add OID Subtree | Specifies a part of the subtree for the selected view | 348 |
| Show OID Subtree | Shows the subtrees assigned to each view | 348 |
| Configure Group | | 351 |
| Add | Adds a group with access policies for assigned users | 351 |
| Show | Shows configured groups and access policies | 351 |
| Configure User | | |
| Add Community | Configures community strings and access mode | 354 |
| Show Community | Shows community strings and access mode | 354 |
| Add SNMPv3 Local User | Configures SNMPv3 users on this switch | 356 |
| Show SNMPv3 Local User | Shows SNMPv3 users configured on this switch | 356 |
| Change SNMPv3 Local User Group | Assign a local user to a new group | 356 |
| Add SNMPv3 Remote User | Configures SNMPv3 users from a remote device | 358 |
| Show SNMPv3 Remote User | Shows SNMPv3 users set from a remote device | 358 |
| Configure Trap | | 360 |
| Add | Configures trap managers to receive messages on key events that occur this switch | 360 |
| Show | Shows configured trap managers | 360 |
| RMON | Remote Monitoring | 364 |
| Configure Global | | |
| Add | | |
| Alarm | Sets threshold bounds for a monitored variable | 365 |
| Event | Creates a response event for an alarm | 367 |
| Show | | |
| Alarm | Shows all configured alarms | 365 |
| Event | Shows all configured events | 367 |
| Configure Interface | | |
| Add | | |
| History | Periodically samples statistics on a physical interface | 369 |
| Statistics | Enables collection of statistics on a physical interface | 372 |

**Table 2: Switch Main Menu (Continued)**

| Menu | Description | Page |
|---|---|---|
| Show | | |
| History | Shows sampling parameters for each entry in the history group | 369 |
| Statistics | Shows sampling parameters for each entry in the statistics group | 372 |
| Show Details | | |
| History | Shows sampled data for each entry in the history group | 369 |
| Statistics | Shows sampled data for each entry in the history group | 372 |
| IP | | |
| General | | |
| Routing Interface | | |
| Add | Configures an IP interface for a VLAN | 417 |
| Show | Shows the IP interfaces assigned to a VLAN | 417 |
| Ping | Sends ICMP echo request packets to another node on the network | 440 |
| Trace Route | Shows the route packets take to the specified destination | 442 |
| ARP | Address Resolution Protocol | 443 |
| Configure General | Sets the protocol timeout, and enables or disables proxy ARP for the specified VLAN | 444 |
| Configure Static Address | | 445 |
| Add | Statically maps a physical address to an IP address | 445 |
| Show | Shows the MAC to IP address static table | 445 |
| Show Information | | |
| Dynamic Address | Shows dynamically learned entries in the IP routing table | 447 |
| Other Address | Shows internal addresses used by the switch | 447 |
| Statistics | Shows statistics on ARP requests sent and received | 448 |
| Routing | | |
| Static Routes | | 449 |
| Add | Configures static routing entries | 449 |
| Show | Shows static routing entries | 449 |
| Modify | Modifies the selected static routing entry | 449 |
| Routing Table | | |
| Show Information | Shows all routing entries, including local, static and dynamic routes | 450 |
| Configure ECMP Number | Sets the maximum number of equal-cost paths to the same destination that can be installed in the routing table | 452 |
| VRRP | Virtual Router Redundancy Protocol | 455 |
| Configure Group ID | | 456 |
| Add | Adds a VRRP group identifier to a VLAN | 456 |
| Show | Shows the VRRP group identifier list | 456 |
| Add IP Address | Sets a virtual interface address for a VRRP group | 456 |

**Table 2: Switch Main Menu (Continued)**

| Menu | Description | Page |
|---|---|---|
| Show IP Addresses | Shows the virtual interface address assigned to a VRRP group | 456 |
| Configure Detail | Configure detailed settings, such as advertisement interval, preemption, priority, and authentication | 456 |
| Show Statistics | | |
| Global Statistics | Displays global statistics for VRRP protocol packet errors | 462 |
| Group Statistics | Displays statistics for VRRP protocol events and errors on the specified VRRP group and interface | 462 |
| IPv6 Configuration | | 420 |
| Configure Global | Sets an IPv6 default gateway for traffic with no known next hop | 421 |
| Configure Interface | Configures IPv6 interface address using auto-configuration or link-local address, and sets related protocol settings | 421 |
| Add IPv6 Address | Adds an global unicast, EUI-64, or link-local IPv6 address to an interface | 424 |
| Show IPv6 Address | Show the IPv6 addresses assigned to an interface | 426 |
| Show IPv6 Neighbor Cache | Displays information in the IPv6 neighbor discovery cache | 428 |
| Show Statistics | | 429 |
| IPv6 | Shows statistics about IPv6 traffic | 429 |
| ICMPv6 | Shows statistics about ICMPv6 messages | 429 |
| UDP | Shows statistics about UDP messages | 429 |
| Show MTU | Shows the maximum transmission unit (MTU) cache for destinations that have returned an ICMP packet-too-big message along with an acceptable MTU to this switch | 435 |
| IP Service | | |
| DNS | Domain Name Service | 465 |
| General | | |
| Configure Global | Enables DNS lookup; defines the default domain name appended to incomplete host names | 465 |
| Add Domain Name | Defines a list of domain names that can be appended to incomplete host names | 466 |
| Show Domain Names | Shows the configured domain name list | 466 |
| Add Name Server | Specifies IP address of name servers for dynamic lookup | 468 |
| Show Name Servers | Shows the name server address list | 468 |
| Static Host Table | | |
| Add | Configures static entries for domain name to address mapping | 469 |
| Show | Shows the list of static mapping entries | 469 |
| Modify | Modifies the static address mapped to the selected host name | 469 |
| Cache | Displays cache entries discovered by designated name servers | 470 |
| DHCP | Dynamic Host Configuration Protocol | 471 |
| Client | Specifies the DHCP client identifier for an interface | 471 |
| Relay | Specifies DHCP relay servers | 472 |

**Table 2: Switch Main Menu (Continued)**

| Menu | Description | Page |
|---|---|---|
| Snooping | | 318 |
| Configure Global | Enables DHCP snooping globally, MAC-address verification, information option; and sets the information policy | 320 |
| Configure VLAN | Enables DHCP snooping on a VLAN | 321 |
| Configure Interface | Sets the trust mode for an interface | 322 |
| Show Information | Displays the DHCP Snooping binding information | 323 |
| Server | | 474 |
| Configure Global | Enables DHCP service on this switch | 474 |
| Configure Excluded Address | | 475 |
| Add | Adds excluded addresses | 475 |
| Show | Shows excluded addresses | 475 |
| Configure Pool | | 476 |
| Add | | 476 |
| Network | Add address pool for network groups | 476 |
| Host | Add address entry for specified host | 476 |
| Show | Shows DHCP pool list | 476 |
| Modify | Modifies the specified pool entry | 476 |
| Show IP Binding | Displays addresses currently bound to DHCP clients | 480 |
| UDP Helper | | 481 |
| General | Enables UDP helper globally on the switch | 481 |
| Forwarding | | 482 |
| Add | Specifies the UDP destination ports for which broadcast traffic will be forwarded | 482 |
| Show | Shows the list of UDP ports to which broadcast traffic will be forwarded | 482 |
| Address | | 483 |
| Add | Specifies the servers to which designated UDP protocol packets are forwarded | 483 |
| Show | Shows the servers to which designated UDP protocol packets are forwarded | 483 |
| Multicast | | 375 |
| IGMP Snooping | | 377 |
| General | Enables multicast filtering; configures parameters for multicast snooping | 379 |
| Multicast Router | | 382 |
| Add Static Multicast Router | Assigns ports that are attached to a neighboring multicast router | 382 |
| Show Static Multicast Router | Displays ports statically configured as attached to a neighboring multicast router | 382 |
| Show Current Multicast Router | Displays ports attached to a neighboring multicast router, either through static or dynamic configuration | 382 |
| IGMP Member | | 384 |

**Table 2: Switch Main Menu (Continued)**

| Menu | Description | Page |
|---|---|---|
| Add Static Member | Statically assigns multicast addresses to the selected VLAN | 384 |
| Show Static Member | Shows multicast addresses statically configured on the selected VLAN | 384 |
| Show Current Member | Shows multicast addresses associated with the selected VLAN, either through static or dynamic configuration | 384 |
| Interface | | |
| Configure VLAN | Configures IGMP snooping per VLAN interface | 386 |
| Show VLAN Information | Shows IGMP snooping settings per VLAN interface | 386 |
| Configure Port | Configures the interface to drop IGMP query packets or all multicast data packets | 391 |
| Configure Trunk | Configures the interface to drop IGMP query packets or all multicast data packets | 391 |
| Forwarding Entry | Displays the current multicast groups learned through IGMP Snooping | 392 |
| Filter | | 393 |
| Configure General | Enables IGMP filtering for the switch | 393 |
| Configure Profile | | 394 |
| Add | Adds IGMP filter profile; and sets access mode | 394 |
| Show | Shows configured IGMP filter profiles | 394 |
| Add Multicast Group Range | Assigns multicast groups to selected profile | 394 |
| Show Multicast Group Range | Shows multicast groups assigned to a profile | 394 |
| Configure Interface | Assigns IGMP filter profiles to port interfaces and sets throttling action | 396 |
| IGMP | Internet Group Management Protocol | 397 |
| Proxy | Configures IGMP proxy service for multicast routing | 398 |
| Interface | Configures Layer 3 IGMP settings for the selected VLAN interface | 401 |
| Static Group | | 403 |
| Add | Configures the router to be a static member of a multicast group on the specified VLAN interface | 403 |
| Show | Shows multicast group statically assigned to a VLAN interface | 403 |
| Group Information | | 405 |
| Show Information | Shows the current multicast groups learned through IGMP for each VLAN | 405 |
| Show Detail | Shows detailed information on each multicast group associated with a VLAN interface | 405 |
| Multicast Routing | | 565 |
| General | Globally enables multicast routing | 568 |
| Information | | 569 |
| Show Summary | Shows each multicast route the switch has learned | 569 |
| Show Detail | Shows additional information for each multicast route the switch has learned, including upstream router, and downstream interfaces | 569 |
| MVR | Multicast VLAN Registration | 408 |
| Configure General | Globally enables MVR, sets the MVR VLAN | 409 |

**Table 2: Switch Main Menu (Continued)**

| Menu | Description | Page |
|---|---|---|
| Configure Group Range | | |
| Add | Configures multicast stream addresses | 410 |
| Show | Shows multicast stream addresses | 410 |
| Configure Interface | Configures MVR interface type and immediate leave status | 411 |
| Configure Static Group Member | | 413 |
| Add | Statically assigns MVR multicast streams to an interface | 413 |
| Show | Show MVR multicast streams statically assigned to an interface | 413 |
| Show Member | Shows information about the interfaces associated with multicast groups assigned to the MVR VLAN | 415 |
| Routing Protocol | | |
| RIP | Routing Information Protocol | 486 |
| General | | 487 |
| Configure | Enables or disables RIP, sets the global RIP attributes and timer values | 487 |
| Clear Route | Clears the specified route type or network interface from the routing table | 490 |
| Network | | 491 |
| Add | Sets the network interfaces that will use RIP | 491 |
| Show | Shows the network interfaces that will use RIP | 491 |
| Passive Interface | | 493 |
| Add | Stops RIP broadcast and multicast messages from being sent on specified network interfaces | 493 |
| Show | Shows the configured passive interfaces | 493 |
| Neighbor Address | | 494 |
| Add | Configures the router to directly exchange routing information with a static neighbor | 494 |
| Show | Shows adjacent hosts or interfaces configured as a neighboring router | 494 |
| Redistribute | | 495 |
| Add | Imports external routing information from other routing domains (that is, protocols) into the autonomous system | 495 |
| Show | Shows the external routing information to be imported from other routing domains | 495 |
| Distance | | 496 |
| Add | Defines an administrative distance for external routes learned from other routing protocols | 496 |
| Show | Shows the administrative distances assigned to external routes learned from other routing protocols | 496 |
| Interface | | 498 |
| Add | Configures RIP parameters for each interface, including send and receive versions, authentication, and method of loopback prevention | 498 |
| Show | Shows the RIP parameters set for each interface | 498 |
| Modify | Modifies RIP parameters for an interface | 498 |
| Statistics | | |

**Table 2: Switch Main Menu (Continued)**

| Menu | Description | Page |
|---|---|---|
| Show Interface Information | Shows RIP settings, and statistics on RIP protocol messages | 502 |
| Show Peer Information | Displays information on neighboring RIP routers | 503 |
| Reset Statistics | Clears statistics for RIP protocol messages | 503 |
| OSPF | Open Shortest Path First (Version 2) | 504 |
| Network Area | | 506 |
| Add | Defines OSPF area address, area ID, and process ID | 506 |
| Show | Shows configured areas | 506 |
| Show Process | Show configured processes | 506 |
| System | | 509 |
| Configure | Configures the Router ID, global settings, and default information | 509 |
| Show | Shows LSA statistics, administrative status, ABR/ASBR, area count, and version number | 511 |
| Area | | 513 |
| Configure Area | | 513 |
| Add Area | Adds NSSA or stub | 513 |
| Show Area | Shows configured NSSA or stub | 513 |
| Configure NSSA Area | Configures settings for importing routes into or exporting routes out of not-so-stubby areas | 514 |
| Configure Stub Area | Configures default cost, and settings for importing routes into a stub | 517 |
| Show Information | Shows statistics for each area, including SPF startups, ABR/ASBR count, LSA count, and LSA checksum | 519 |
| Area Range | | 520 |
| Add | Configures route summaries to advertise at an area boundary | 520 |
| Show | Shows route summaries advertised at an area boundary | 520 |
| Modify | Modifies route summaries advertised at an area boundary | 520 |
| Redistribute | | 522 |
| Add | Redistributes routes from one routing domain to another | 522 |
| Show | Shows route types redistributed to another domain | 522 |
| Modify | Modifies configuration settings for redistributed routes | 522 |
| Summary Address | | 524 |
| Add | Aggregates routes learned from other protocols for advertising into other autonomous systems | 524 |
| Show | Shows configured summary addresses | 524 |
| Interface | | 525 |
| Show | Shows area ID and designated router settings for each interface | 525 |
| Configure by VLAN | Configures OSPF protocol settings and authentication for specified VLAN | 525 |
| Configure by Address | Configures OSPF protocol settings and authentication for specified interface address | 525 |
| Show MD5 Key | Shows MD5 key ID used for each area | 525 |

**Table 2: Switch Main Menu (Continued)**

| Menu | Description | Page |
|---|---|---|
| Virtual Link | | 531 |
| Add | Configures a virtual link through a transit area to the backbone | 531 |
| Show | Shows virtual links, neighbor address, and state | 531 |
| Configure Detailed Settings | Configures detailed protocol and authentication settings | 531 |
| Show MD5 Key | Shows the MD5 key ID used for each neighbor | 531 |
| Information | | |
| LSDB | Shows information about different OSPF Link State Advertisements (LSAs) | 534 |
| Neighbor | Shows information about each OSPF neighbor | 536 |
| OSPFv3 | Open Shortest Path First (Version 3) | 537 |
| General | | 539 |
| Add | Creates an OSPFv3 routing process | 539 |
| Show | Shows the configured OSPFv3 routing processes | 539 |
| Tag | | 540 |
| Configure | Configures general protocol settings for OSPF | 540 |
| Show | Shows administrative settings and statistics for OSPF | 540 |
| Configure Passive Interface | Suppresses OSPF routing traffic on a specified interface | 544 |
| Area | Configures stubs | 545 |
| Configure Area | | 545 |
| Add Area | Adds a stubby area | 545 |
| Show Area | Shows the protocol settings for all stubs | 545 |
| Configure Area | Configures protocol settings for an existing stub | 545 |
| Show Information | Displays protocol information on stubs | 547 |
| Area Range | Configures an ABR to advertise a single summary route that covers all the individual networks within its area | 548 |
| Add | Adds a summary route that covers all the individual networks within an area | 548 |
| Show | Shows the summary routes configured for individual networks within an area | 548 |
| Modify | Modifies the advertising parameter for summary routes | 548 |
| Virtual Link | | 550 |
| Add | Adds a virtual link from an area that does not have a direct physical connection to the OSPF backbone | 550 |
| Show | Shows the virtual links configured on this router | 550 |
| Configure Detailed Settings | Configures detailed settings for existing virtual links | 550 |
| Interface | Configures interface-specific parameters used by OSPF | 553 |
| Show Area | Shows the OSPF areas bound to an interface | 553 |
| Add Area | Binds an OSPF area to a Layer 3 interface | 553 |
| Configure | Configures OSPF protocol settings for a Layer 3 interface | 553 |

**Table 2: Switch Main Menu (Continued)**

| Menu | Description | Page |
|---|---|---|
| Modify Detailed Settings | Modifies the OSPF protocol settings for a Layer 3 interface | 553 |
| Show | Shows the status of OSPFv3 interfaces | 557 |
| Show Counters | Shows information on neighboring routers and the exchange of protocol messages for OSPFv3 interfaces | 559 |
| Information | | |
| Neighbor | Displays information about neighboring routers on each interface | 560 |
| Virtual Neighbor | Shows information about the neighbor router assigned to the other end of a virtual link | 561 |
| Route | Shows the OSPF routing table | 562 |
| Virtual Link | Shows the Link State Advertisements (LSAs) stored in the link state database for virtual links | 563 |
| PIM | Protocol Independent Multicasting | 572 |
| General | Enables PIM globally for the switch | 572 |
| Interface | Enables PIM per interface, and sets the mode to dense or sparse | 572 |
| Neighbor | Displays information neighboring PIM routers | 578 |
| PIM-SM | Protocol Independent Multicasting – Sparse Mode | |
| Configure Global | Configures settings for register messages, and use of the SPT | 578 |
| BSR Candidate | Configures the switch as a BSR candidate | 580 |
| RP Address | | 581 |
| Add | Sets a static address for an RP and the associated multicast group(s) | 581 |
| Show | Shows the static addresses configured for each RP and the associated multicast groups | 581 |
| RP Candidate | | 583 |
| Add | Advertises the switch as an RP candidate to the BSR for the specified multicast groups | 583 |
| Show | Shows the multicast groups for which this switch is advertising itself as an RP candidate to the BSR | 583 |
| Show Information | | |
| Show BSR Router | Displays information about the BSR | 585 |
| Show RP Mapping | Displays the active RPs and associated multicast routing entries | 586 |
| PIM6 | PIM for IPv6 | |
| General | Enables PIM globally for the switch | 587 |
| Interface | Enables PIM per interface, and sets the mode to dense or sparse | 588 |
| Neighbor | Displays information neighboring PIM routers | 591 |

# 4 BASIC MANAGEMENT TASKS

This chapter describes the following topics:

- Displaying System Information – Provides basic system description, including contact information.
- Displaying Switch Hardware/Software Versions – Shows the hardware version, power status, and firmware versions
- Configuring Support for Jumbo Frames – Enables support for jumbo frames.
- Displaying Bridge Extension Capabilities – Shows the bridge extension parameters.
- Managing System Files – Describes how to upgrade operating software or configuration files, and set the system start-up files.
- Setting the System Clock – Sets the current time manually or through specified SNTP servers.
- Console Port Settings – Sets console port connection parameters.
- Telnet Settings – Sets Telnet connection parameters.
- Displaying CPU Utilization – Displays information on CPU utilization.
- Displaying Memory Utilization – Shows memory utilization parameters.
- Resetting the System – Restarts the switch immediately, at a specified time, after a specified delay, or at a periodic interval.

## DISPLAYING SYSTEM INFORMATION

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

### CLI REFERENCES

- "System Management Commands" on page 615
- "SNMP Commands" on page 659

### PARAMETERS

These parameters are displayed in the web interface:

- **System Description** – Brief description of device type.
- **System Object ID** – MIB II object ID for switch's network management subsystem.

■**System Up Time** – Length of time the management agent has been up.

■**System Name** – Name assigned to the switch system.

■**System Location** – Specifies the system location.

■**System Contact** – Administrator responsible for the system.

### WEB INTERFACE

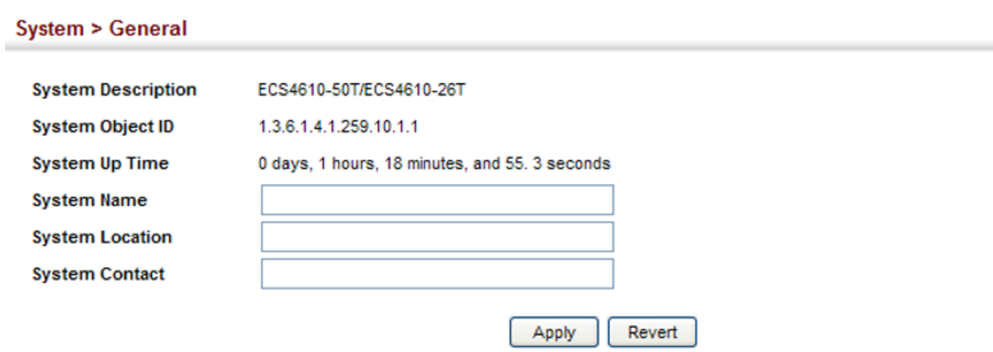
To configure general system information:

1. Click System, General.

2. Specify the system name, location, and contact information for the system administrator.

3. Click Apply.

**Figure 1: System Information**




## DISPLAYING SWITCH HARDWARE/SOFTWARE VERSIONS

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

### CLI REFERENCES

■"System Management Commands" on page 615

### PARAMETERS

The following parameters are displayed in the web interface:

*Main Board Information*

■**Serial Number** – The serial number of the switch.

■**Number of Ports** – Number of built-in ports.

■**Hardware Version** – Hardware version of the main board.

- **Internal Power Status** – Displays the status of the internal power supply.

*Management Software Information*

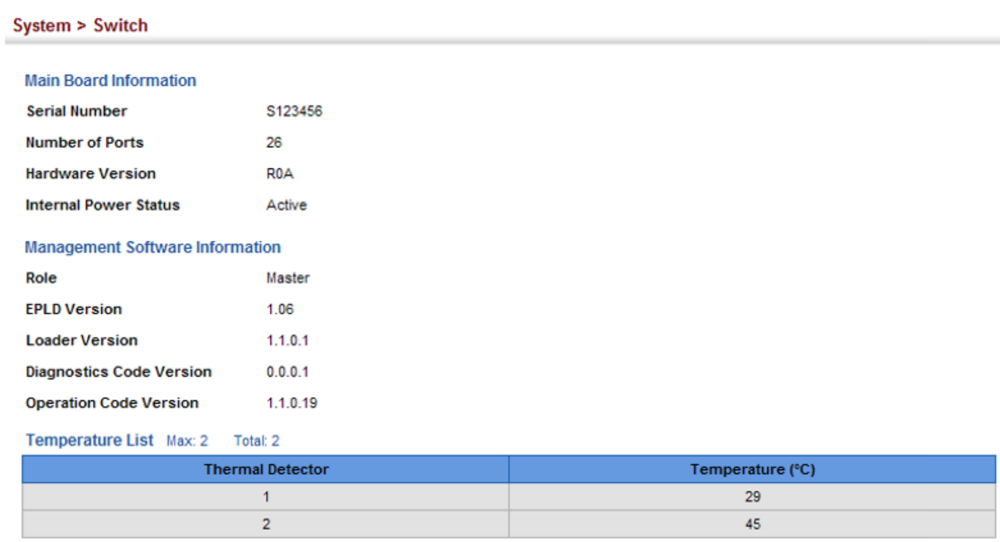
- **Role** – Shows that this switch is operating as Master or Slave.
- **EPLD Version** – Version number of EEPROM Programmable Logic Device.
- **Loader Version** – Version number of loader code.
- **Diagnostics Code Version** – Version of Power-On Self-Test (POST) and boot code.
- **Operation Code Version** – Version number of runtime code.
- **Thermal Detector** – The first detector is near the air flow intake vents on both models. The second detector is near the switch ASIC on the EL326.
- **Temperature** – Temperature at specified thermal detection point.

### WEB INTERFACE

To view hardware and software version information.

1. Click System, then Switch.

**Figure 2: General Switch Information**



## CONFIGURING SUPPORT FOR JUMBO FRAMES

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

### CLI REFERENCES

■"System Management Commands" on page 615

### USAGE GUIDELINES

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

### PARAMETERS

The following parameters are displayed in the web interface:

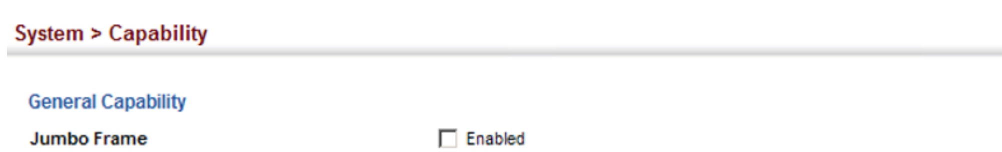
■**Jumbo Frame** – Configures support for jumbo frames. (Default: Disabled)

### WEB INTERFACE

To configure support for jumbo frames:

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

**Figure 3: Configuring Support for Jumbo Frames**



## DISPLAYING BRIDGE EXTENSION CAPABILITIES

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

### CLI REFERENCES

- "GVRP and Bridge Extension Commands" on page 886

### PARAMETERS

The following parameters are displayed in the web interface:

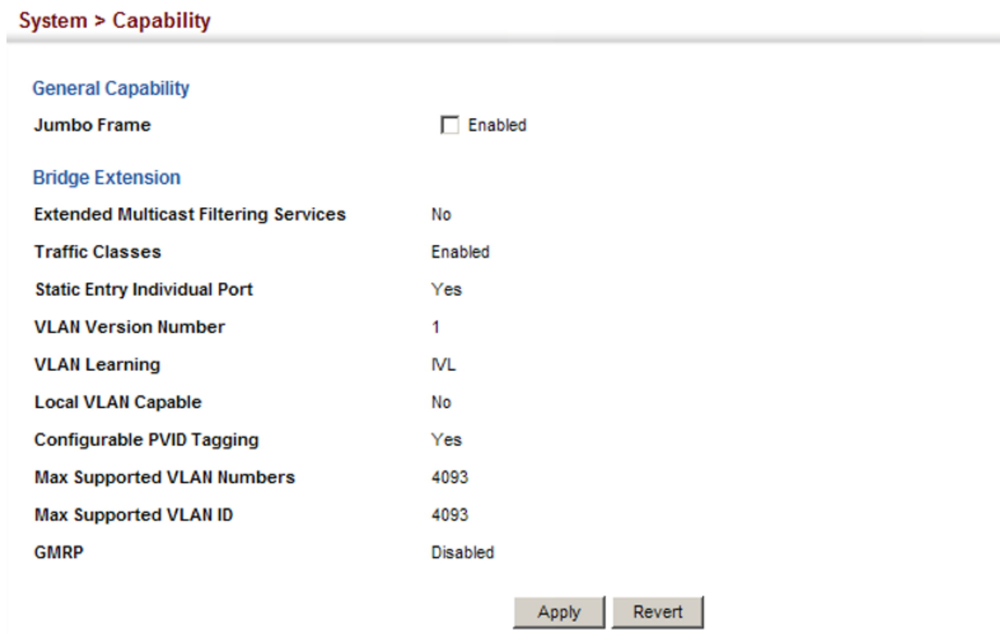
- **Extended Multicast Filtering Services** – This switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).
- **Traffic Classes** – This switch provides mapping of user priorities to multiple traffic classes. (Refer to "Class of Service" on page 203.)
- **Static Entry Individual Port** – This switch allows static filtering for unicast and multicast addresses. (Refer to "Setting Static Addresses" on page 170.)
- **VLAN Version Number** – Based on IEEE 802.1Q, “1” indicates Bridges that support only single spanning tree (SST) operation, and “2” indicates Bridges that support multiple spanning tree (MST) operation.
- **VLAN Learning** – This switch uses Independent VLAN Learning (IVL), where each port maintains its own filtering database.
- **Local VLAN Capable** – This switch does not support multiple local bridges outside of the scope of 802.1Q defined VLANs.
- **Configurable PVID Tagging** – This switch allows you to override the default Port VLAN ID (PVID used in frame tags) and egress status (VLAN-Tagged or Untagged) on each port. (Refer to "VLAN Configuration" on page 137.)
- **Max Supported VLAN Numbers** – The maximum number of VLANs supported on this switch.
- **Max Supported VLAN ID** – The maximum configurable VLAN identifier supported on this switch.
- **GMRP** – GARP Multicast Registration Protocol (GMRP) allows network devices to register end stations with multicast groups. This switch does not support GMRP; it uses the Internet Group Management Protocol (IGMP) to provide automatic multicast filtering.

### WEB INTERFACE

To view Bridge Extension information:

1. Click System, then Capability.

**Figure 4: Displaying Bridge Extension Configuration**




## MANAGING SYSTEM FILES

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

### Copying Files via FTP/TFTP or HTTP

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

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

**CLI REFERENCES**

■ "copy" on page 625

**PARAMETERS**

The following parameters are displayed in the web interface:

■ **Copy Type** – The firmware copy operation includes these options:

- FTP Upgrade – Copies a file from an FTP server to the switch.
- FTP Download – Copies a file from the switch to an FTP server.

- HTTP Upgrade – Copies a file from a management station to the switch.
- HTTP Download – Copies a file from the switch to a management station
- TFTP Upgrade – Copies a file from a TFTP server to the switch.
- TFTP Download – Copies a file from the switch to a TFTP server.

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

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

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

■ **File Type** – Specify Operation Code to copy firmware.

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

---

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

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

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

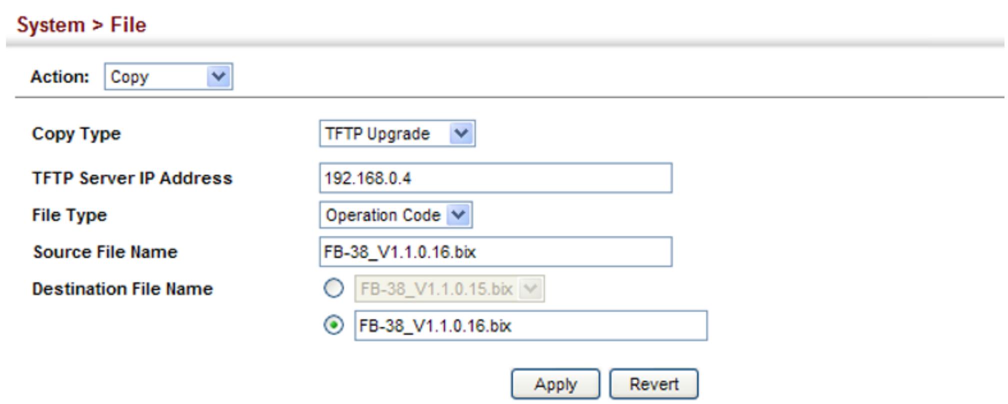
---

**WEB INTERFACE**

To copy firmware files:

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

**Figure 5: Copy Firmware**




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

## Saving the Running Configuration to a Local File

Use the System > File (Copy) page to save the current configuration settings to a local file on the switch. The configuration settings are not automatically saved by the system for subsequent use when the switch is rebooted. You must save these settings to the current startup file, or to another file which can be subsequently set as the startup file.

### CLI REFERENCES

■"copy" on page 625

### PARAMETERS

The following parameters are displayed in the web interface:

■**Copy Type** – The copy operation includes this option:

- ◆ Running-Config – Copies the current configuration settings to a local file on the switch.

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

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

### WEB INTERFACE

To save the running configuration file:

1. Click System, then File.

2. Select Copy from the Action list.

3. Select Running-Config from the Copy Type list.

4. Select the current startup file on the switch to overwrite or specify a new file name.

5. Then click Apply.

**Figure 6: Saving the Running Configuration**


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

## Setting The Start-Up File

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

### CLI REFERENCES

- "whichboot" on page 630
- "boot system" on page 625

### WEB INTERFACE

To set a file to use for system initialization:

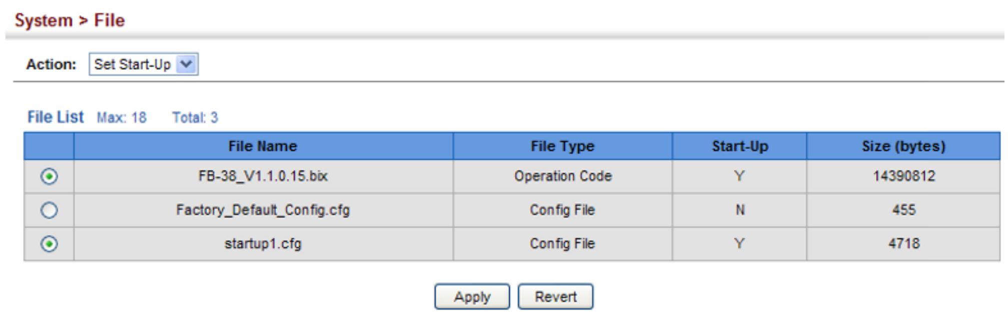
1. Click System, then File.

2. Select Set Start-Up from the Action list.

3. Mark the operation code or configuration file to be used at startup

4. Then click Apply.

**Figure 7: Setting Start-Up Files**




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

## Showing System Files

Use the System > File (Show) page to show the files in the system directory, or to delete a file.

NOTE: Files designated for start-up, and the Factory_Default_Config.cfg file, cannot be deleted.

### CLI REFERENCES

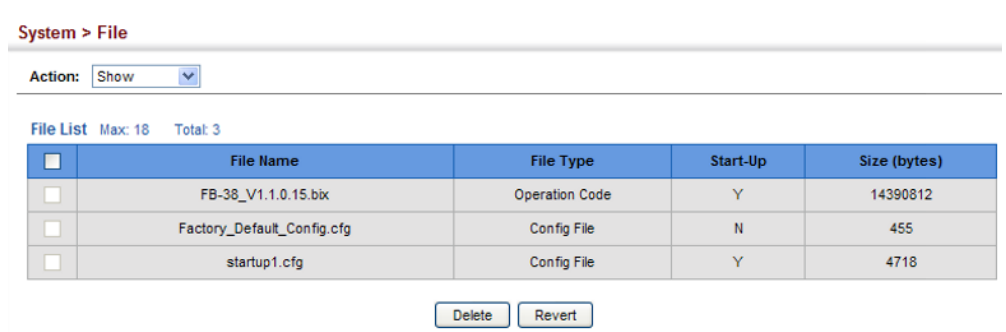
■ "dir" on page 629
■ "delete" on page 628

### WEB INTERFACE

To show the system files:

1. Click System, then File.
2. Select Show from the Action list.
3. To delete a file, mark it in the File List and click Delete.

**Figure 8: Displaying System Files**



# SETTING THE SYSTEM CLOCK

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

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

## Setting the Time Manually

Use the System > Time (Configure General - Manual) page to set the system time on the switch manually without using SNTP.

### CLI REFERENCES

■"calendar set" on page 653
■"show calendar" on page 654

### PARAMETERS

The following parameters are displayed in the web interface:

■**Current Time** – Shows the current time set on the switch.

■**Hours** – Sets the hour. (Range: 0-23; Default: 0)

■**Minutes** – Sets the minute value. (Range: 0-59; Default: 0)

■**Seconds** – Sets the second value. (Range: 0-59; Default: 0)

■**Month** – Sets the month. (Range: 1-12; Default: 1)

■**Day** – Sets the day of the month. (Range: 1-31; Default: 1)

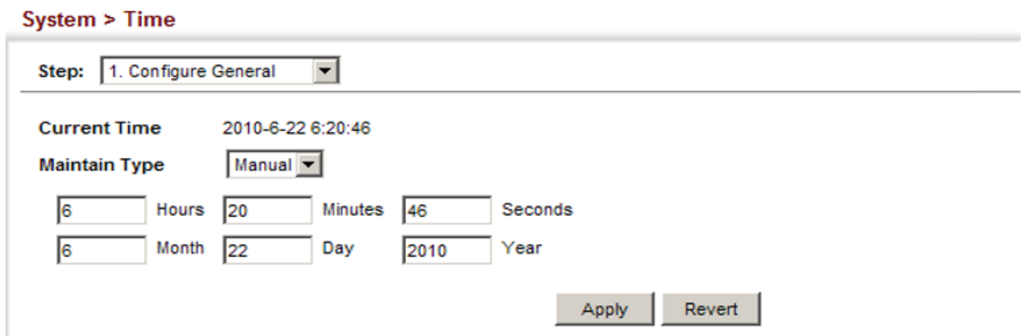
■**Year** – Sets the year. (Range: 2001-2100; Default: 2009)

### WEB INTERFACE

To manually set the system clock:

1. Click System, then Time.
2. Select Configure General from the Action list.
3. Select Manual from the Maintain Type list.
4. Enter the time and date in the appropriate fields.
5. Click Apply

**Figure 9: Manually Setting the System Clock**




## Configuring SNTP

Use the System > Time (Configure General - SNTP) page to configure the switch to send time synchronization requests to time servers. Set the SNTP polling interval, SNTP servers, and also the time zone.

### CLI References

- "Time" on page 649

### Setting the Polling Interval

Specify the polling interval at which the switch will query the time servers.

#### Parameters

The following parameters are displayed in the web interface:

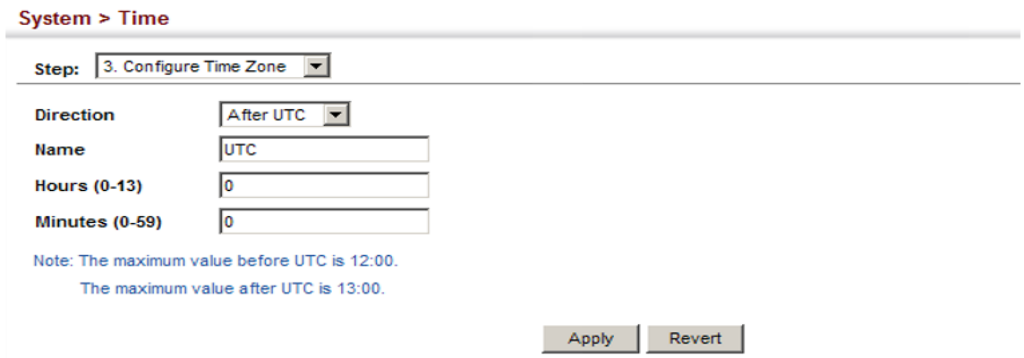
- **Current Time** – Shows the current time set on the switch.
- **SNTP Polling Interval** – Sets the interval between sending requests for a time update from a time server. (Range: 16-16384 seconds; Default: 16 seconds)

#### Web Interface

To set the polling interval for SNTP:

1. Click System, then Time.
2. Select Configure General from the Action list.
3. Select SNTP from the Maintain Type list.
4. Modify the polling interval if required.
5. Click Apply

**Figure 10: Setting the Polling Interval for SNTP**




## Specifying SNTP Time Servers

Use the System > Time (Configure Time Server) page to specify the IP address for up to three SNTP time servers.

### CLI REFERENCES

- "sntp server" on page 651

### PARAMETERS

The following parameters are displayed in the web interface:

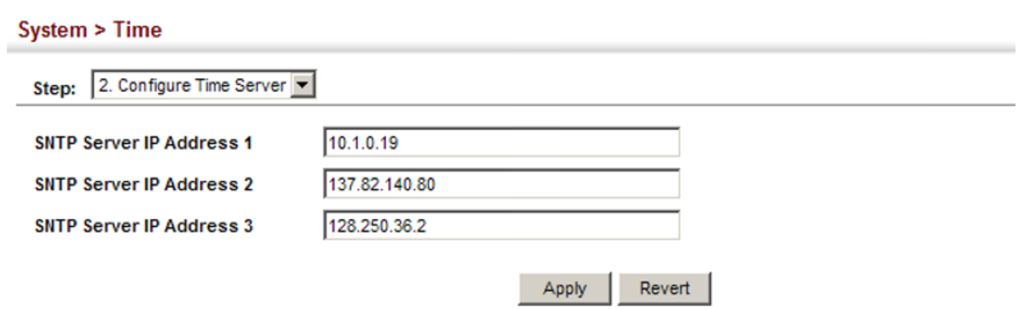
- **SNTP Server IP Address** – Sets the IPv4 or IPv6 address for up to three time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence.

### WEB INTERFACE

To set the SNTP time servers:

1. Click System, then Time.
2. Select Configure Time Server from the Action list.
3. Enter the IP address of up to three time servers.
4. Click Apply.

**Figure 11: Specifying SNTP Time Servers**



## Setting the Time Zone

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

### Parameters

The following parameters are displayed in the web interface:

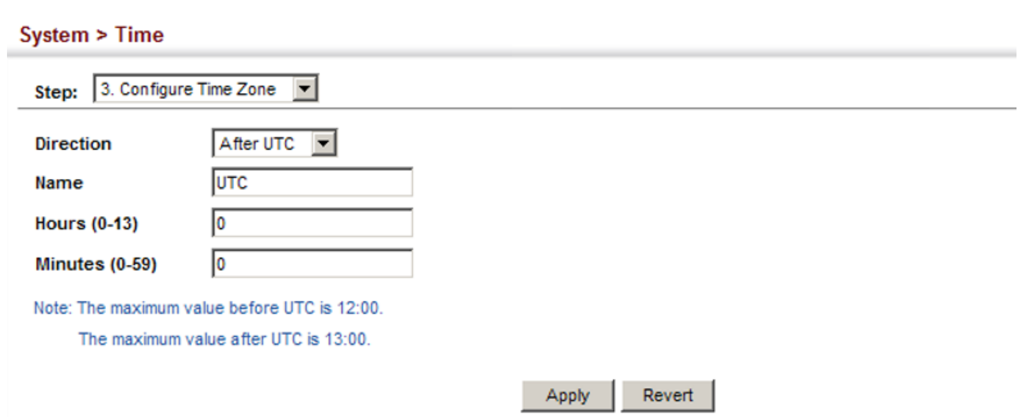
- **Direction**: Configures the time zone to be before (east of) or after (west of) UTC.
- **Name** – Assigns a name to the time zone. (Range: 1-29 characters)
- **Hours** (0-13) – The number of hours before/after UTC. The maximum value before UTC is 12. The maximum value after UTC is 13.
- **Minutes** (0-59) – The number of minutes before/after UTC.

### Web Interface

To set your local time zone:

1. Click System, then Time.
2. Select Configure Time Zone from the Action list.
3. Set the offset for your time zone relative to the UTC in hours and minutes.
4. Click Apply.

**Figure 12: Setting the Time Zone**




## Console Port Settings

Use the System > Console menu to configure connection parameters for the switch's console port. You can access the onboard configuration program by attaching a

VT100 compatible device to the switch's serial console port. Management access through the console port is controlled by various parameters, including a password (only configurable through the CLI), time outs, and basic communication settings. Note that these parameters can be configured via the web or CLI interface.

### CLI REFERENCES

■ "Line" on page 630

### PARAMETERS

The following parameters are displayed in the web interface:

- **Login Timeout** – Sets the interval that the system waits for a user to log into the CLI. If a login attempt is not detected within the timeout interval, the connection is terminated for the session. (Range: 0-300 seconds; Default: 0 seconds)

- **Exec Timeout** – Sets the interval that the system waits until user input is detected. If user input is not detected within the timeout interval, the current session is terminated. (Range: 0-65535 seconds; Default: 600 seconds)

- **Password Threshold** – Sets the password intrusion threshold, which limits the number of failed logon attempts. When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time (set by the Silent Time parameter) before allowing the next logon attempt.
(Range: 0-120; Default: 3 attempts)

- **Quiet Period** – Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts has been exceeded.
(Range: 0-65535 seconds; Default: Disabled)

- **Data Bits** – Sets the number of data bits per character that are interpreted and generated by the console port. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character. (Default: 8 bits)

- **Stop Bits** – Sets the number of the stop bits transmitted per byte. (Range: 1-2; Default: 1 stop bit)

- **Parity** – Defines the generation of a parity bit. Communication protocols provided by some terminals can require a specific parity bit setting. Specify Even, Odd, or None. (Default: None)

- **Speed** – Sets the terminal line's baud rate for transmit (to terminal) and receive (from terminal). Set the speed to match the baud rate of the device connected to the serial port. (Range: 9600, 19200, 38400, 57600, or 115200 baud;
Default: 115200 baud)

---

NOTE: The password for the console connection can only be configured through the CLI (see "password" on page 635).

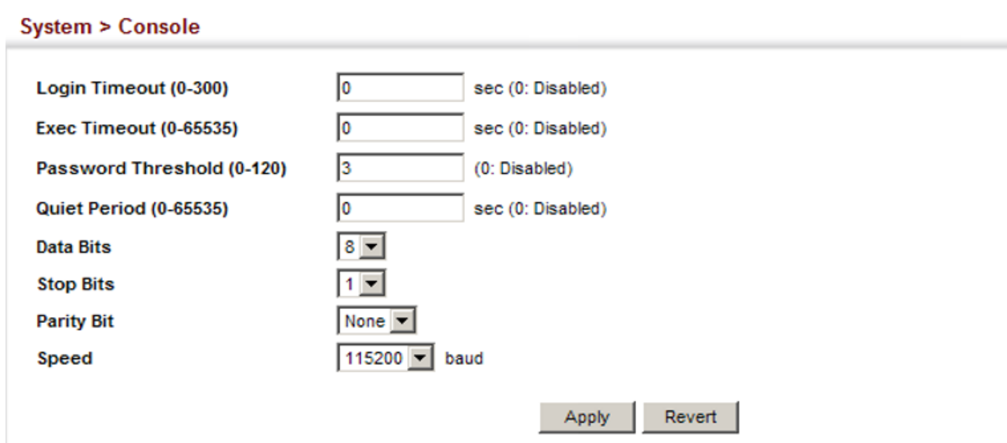
NOTE: Password checking can be enabled or disabled for logging in to the console connection (see "login" on page 633). You can select authentication by a single global password as configured for the password command, or by passwords set up for specific user-name accounts. The default is for local passwords configured on the switch.

### WEB INTERFACE

To configure parameters for the console port:

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

**Figure 13: Console Port Settings**




## TELNET SETTINGS

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

### CLI REFERENCES

- "Line" on page 630

### PARAMETERS

The following parameters are displayed in the web interface:

- **Telnet Status** – Enables or disables Telnet access to the switch. (Default: Enabled)
- **TCP Port** – 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)

- **Quiet Period** – Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts has been exceeded.
  (Range: 0-65535 seconds; Default: Disabled)

---

NOTE: The password for the Telnet connection can only be configured through the CLI (see "password" on page 635).

NOTE: Password checking can be enabled or disabled for login to the console connection (see "login" on page 633). You can select authentication by a single global password as configured for the password command, or by passwords set up for specific user-name accounts. The default is for local passwords configured on the switch.

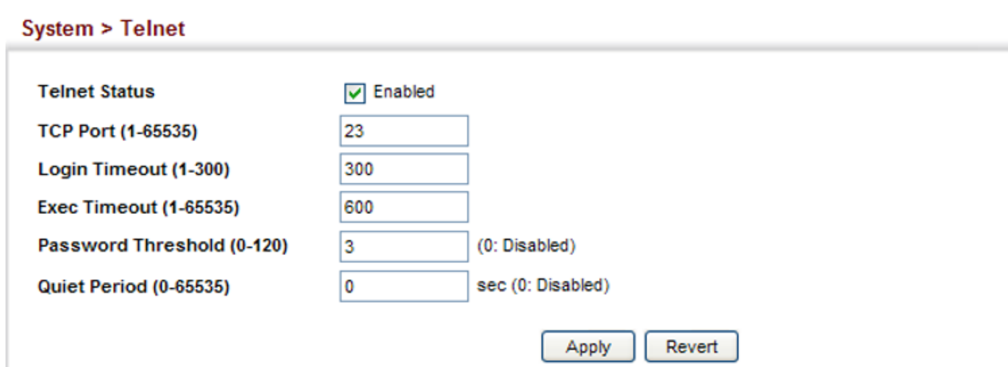
---

### WEB INTERFACE

To configure parameters for the console port:

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

**Figure 14: Telnet Connection Settings**



## DISPLAYING CPU UTILIZATION

Use the System > CPU Utilization page to display information on CPU utilization.

### CLI REFERENCES

■"show process cpu" on page 617

### PARAMETERS

The following parameters are displayed in the web interface:

■**Time Interval** – The interval at which to update the displayed utilization rate. (Options: 1, 5, 10, 30, 60 seconds; Default: 1 second)

■**CPU Utilization** – CPU utilization over specified interval.

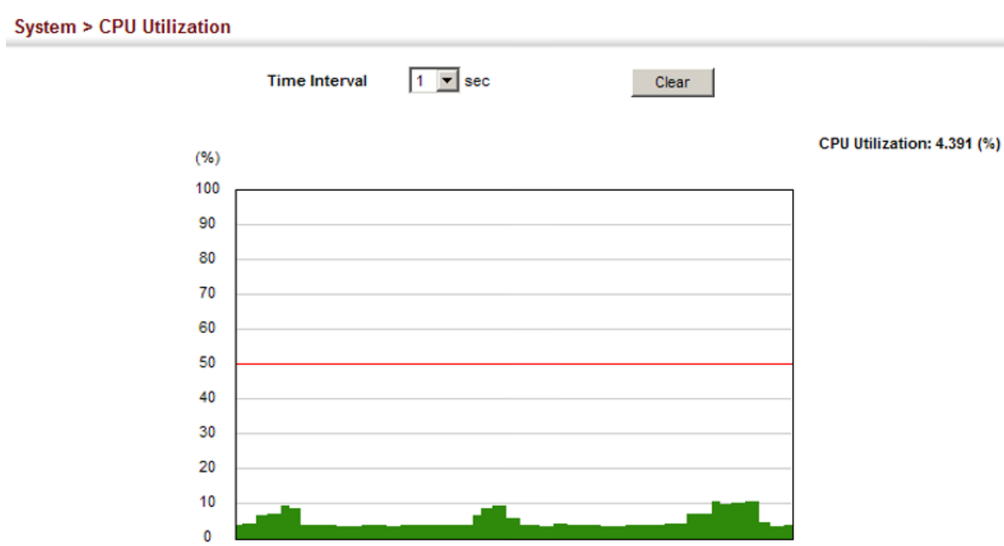
### WEB INTERFACE

To display CPU utilization:

1. Click System, then CPU Utilization.

2. Change the update interval if required. Note that the interval is changed as soon as a new setting is selected.

**Figure 15: Displaying CPU Utilization**




## DISPLAYING MEMORY UTILIZATION

Use the System > Memory Status page to display memory utilization parameters.

### CLI REFERENCES

■"show memory" on page 617

### PARAMETERS

The following parameters are displayed in the web interface:

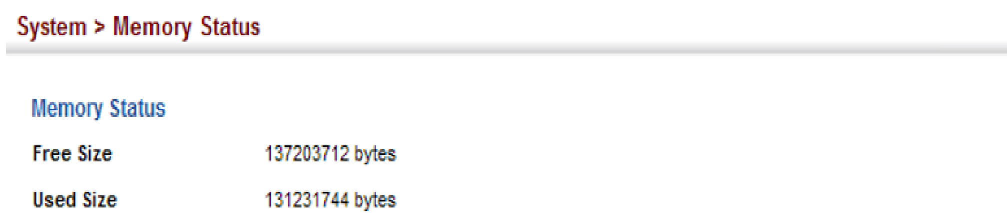
- **Free Size** – The amount of memory currently free for use.
- **Used Size** – The amount of memory allocated to active processes.
- **Total** – The total amount of system memory.

### WEB INTERFACE

To display memory utilization:

1. Click System, then Memory Status.

**Figure 16: Displaying Memory Utilization**




## RESETTING THE SYSTEM

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

### CLI REFERENCES

- "reload (Privileged Exec)" on page 612
- "reload (Global Configuration)" on page 608
- "show reload" on page 612

### COMMAND USAGE

- This command resets the entire system.
- When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory by the copy running-config startup-config command (See "copy" on page 625).

### PARAMETERS

The following parameters are displayed in the web interface:

*System Reload Configuration*

- **Reset Mode** – Restarts the switch immediately or at the specified time(s).
  - **Immediately** – Restarts the system immediately.

- **In** – Specifies an interval after which to reload the switch. (The specified time must be equal to or less than 24 days.)
  - *hours* – The number of hours, combined with the minutes, before the switch resets. (Range: 0-576)
  - *minutes* – The number of minutes, combined with the hours, before the switch resets. (Range: 0-59)
- **At** – Specifies a periodic interval at which to reload the switch.
  - DD - The day of the month at which to reload. (Range: 1-31)
  - MM - The month at which to reload. (january ... december)
  - YYYY - The year at which to reload. (Range: 2001-2050)
  - HH - The hour at which to reload. (Range: 0-23)
  - MM - The minute at which to reload. (Range: 0-59)
- **Regularly** – Specifies a periodic interval at which to reload the switch.

  *Time*
  - HH - The hour at which to reload. (Range: 0-23)
  - MM - The minute at which to reload. (Range: 0-59)

  *Period*
  - Daily - Every day.
  - Weekly - Day of the week at which to reload. (Range: Sunday ... Saturday)
  - Monthly - Day of the month at which to reload. (Range: 1-31)

**WEB INTERFACE**
To restart the switch:

1. Click System, then Reset.
2. Select the required rest mode.
3. For any option other than to reset immediately, fill in the required parameters
4. Click Apply.
5. When prompted, confirm that you want reset the switch.

**Figure 17: Restarting the Switch** (Immediately)

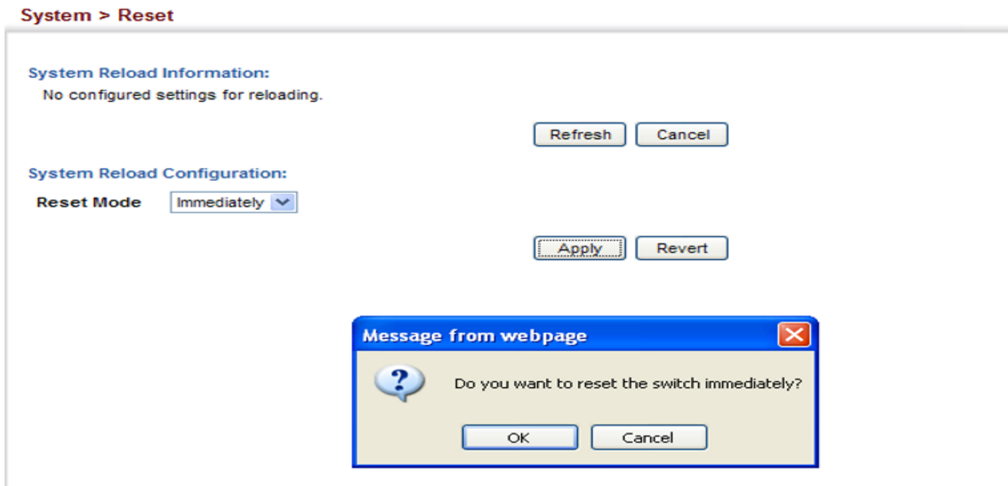



**Figure 18: Restarting the Switch** (In)

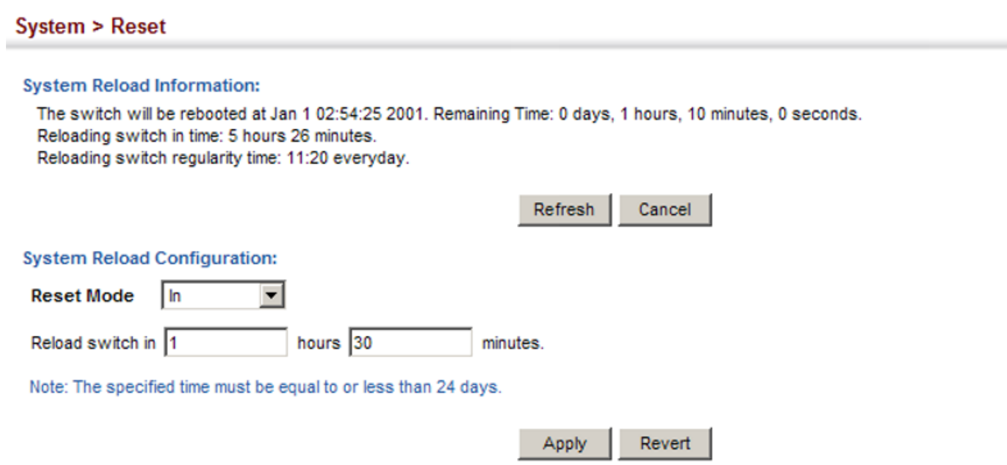


**Figure 19: Restarting the Switch** (At)

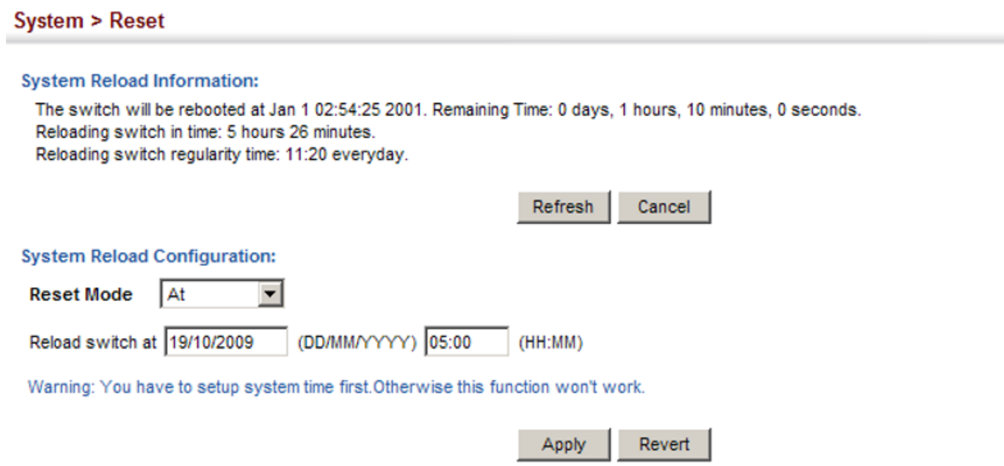
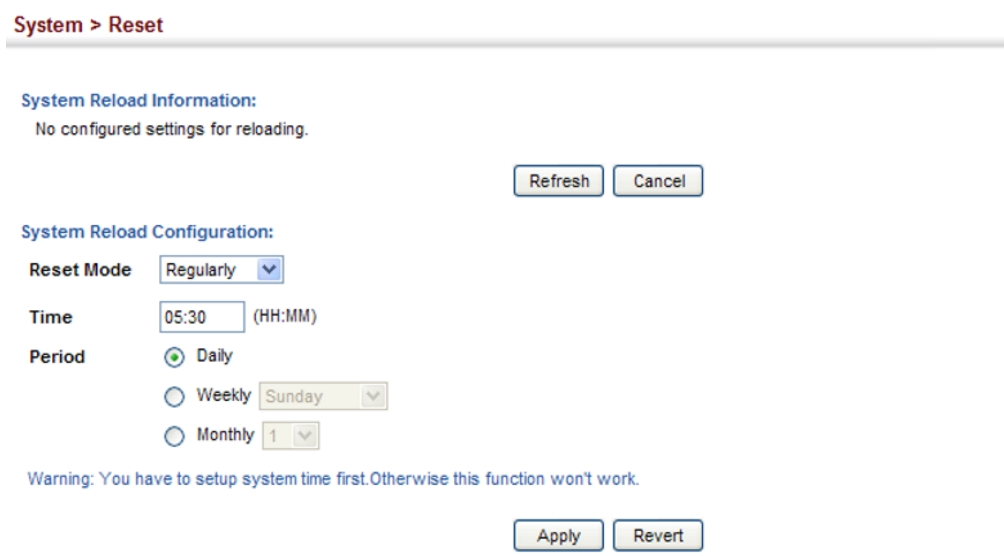



**Figure 20: Restarting the Switch** (Regularly)



# 5 INTERFACE CONFIGURATION

This chapter describes the following topics:

- Port Configuration – Configures connection settings, including auto-negotiation, or manual setting of speed, duplex mode, and flow control.
- Port Mirroring – Sets the source and target ports for mirroring on the local switch.
- Displaying Statistics – Shows Interface, Etherlike, and RMON port statistics in table or chart form.
- Cable Test – Performs cable diagnostics on the specified port.
- Trunk Configuration – Configures static or dynamic trunks.
- Flow Sampling – Configures periodic sampling of traffic flows.
- Traffic Segmentation – Configures the uplinks and down links to a segmented group of ports.
- VLAN Trunking – Configures a tunnel across one or more intermediate switches which pass traffic for VLAN groups to which they do not belong.

## PORT CONFIGURATION

This section describes how to configure port connections, mirror traffic from one port to another, and run cable diagnostics.

### Configuring by Port List

Use the Interface > Port > General (Configure by Port List) page to enable/disable an interface, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed, duplex mode, and flow control.

#### CLI REFERENCES

- Interface Commands on page 784

#### COMMAND USAGE

- Auto-negotiation must be disabled before you can configure or force a Gigabit RJ-45 interface to use the Speed/Duplex mode or Flow Control options.
- When using auto-negotiation, the optimal settings will be negotiated between the link partners based on their advertised capabilities. To set the speed, duplex mode, or flow control under auto-negotiation, the required operation modes must be specified in the capabilities list for an interface.

- The 1000BASE-T and 10GBASE-T standard does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T or 10GBASE-T port or trunk. If not used, the success of the link process cannot be guaranteed when connecting to other types of switches.

- The Speed/Duplex mode is fixed at 1000full on the Gigabit SFP ports, and at 10Gfull on the 10 Gigabit ports. When auto-negotiation is enabled, the only attributes which can be advertised include flow control and symmetric pause frames.

**PARAMETERS**

These parameters are displayed in the web interface:

- **Port** – Port identifier.

- **Type** – Indicates the port type. (1000Base-T, 1000Base SFP, or 10G)

- **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.

- **Media Type** – Configures the forced/preferred port type to use for the combination ports.

  - **Copper-Forced** - Always uses the built-in RJ-45 port.

  - **SFP-Forced** - Always uses the SFP port, even if a module is not installed.

  - **SFP-Preferred-Auto** - Uses SFP port if both combination types are functioning and the SFP port has a valid link. (This is the default for Ports 21-26/45-50.)

- **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.

  - **10h** - Supports 10 Mbps half-duplex operation

  - **10f** - Supports 10 Mbps full-duplex operation

  - **100h** - Supports 100 Mbps half-duplex operation

  - **100f** - Supports 100 Mbps full-duplex operation

  - **1000f** (Gigabit ports only) - Supports 1000 Mbps full-duplex operation

  - **10Gf** (10 Gigabit ports only) - Supports 10 Gbps full-duplex operation

  - **Sym** - Check this item to transmit and receive pause frames.

- **FC** - Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3-2005 (formally IEEE 802.3x) for full-duplex operation.

  Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.

  (Default: Autonegotiation enabled on Gigabit and 10 Gigabit ports; Advertised capabilities for
  1000BASE-T – 10half, 10full, 100half, 100full, 1000full;
  1000Base-SX/LX/LH – 1000full
  10GBASE-SR/LR/ER - 10Gfull
  10GBASE-T - 10Gfull)

■ **Speed/Duplex** – Allows you to manually set the port speed and duplex mode. (i.e., with auto-negotiation disabled)

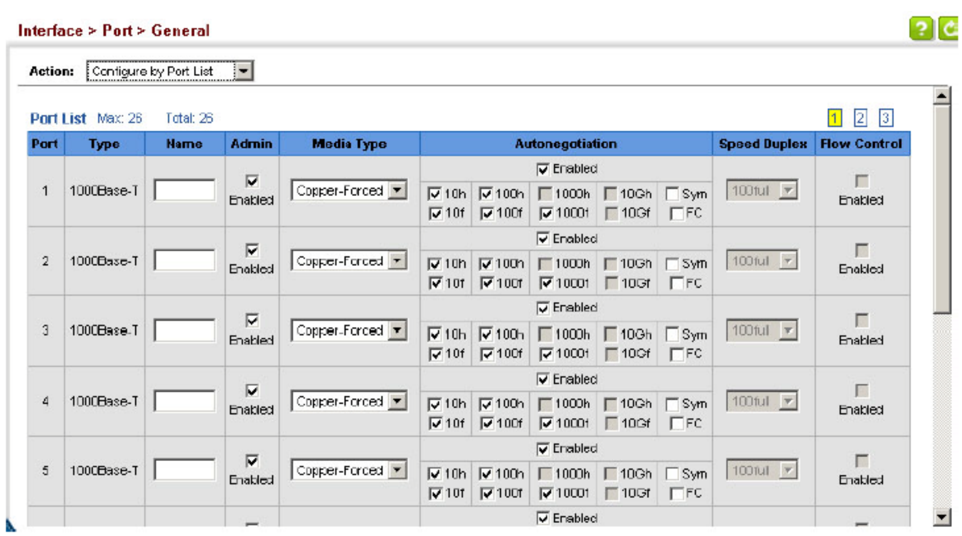
■ **Flow Control** – Allows automatic or manual selection of flow control.

### WEB INTERFACE

To configure port connection parameters:

1. Click Interface, Port, General.
2. Select Configure by Port List from the Action List.
3. Modify the required interface settings.
4. Click Apply.

**Figure 1: Configuring Connections by Port List**



## Configuring by Port Range

Use the Interface > Port > General (Configure by Port Range) 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.

For more information on command usage and a description of the parameters, refer to "Configuring by Port List" on page 107.

### CLI REFERENCES

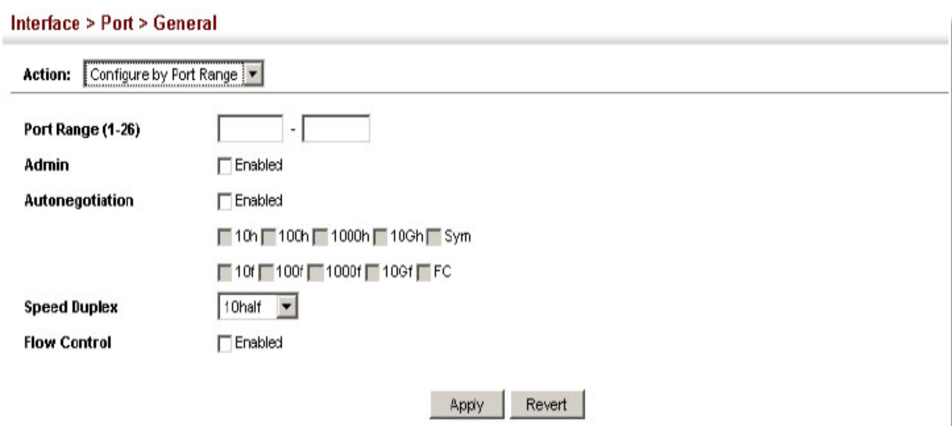
- "Interface Commands" on page 805

### WEB INTERFACE

To configure port connection parameters:

1. Click Interface, Port, General.
2. Select Configure by Port Range from the Action List.
3. Enter to range of ports to which your configuration changes apply.
4. Modify the required interface settings.
5. Click Apply.

**Figure 2: Configuring Connections by Port Range**




## Displaying Connection Status

Use the Interface > Port > General (Show Information) page to display the current connection status, including link state, speed/duplex mode, flow control, and auto-negotiation.

### CLI REFERENCES

- "show interfaces status" on page 816

### PARAMETERS

These parameters are displayed in the web interface:

- **Port** – Port identifier.

■**Type** – Indicates the port type. (1000Base-T, 1000Base SFP, or 10G)

■**Name** – Interface label.

■**Admin** – Shows if the port is enabled or disabled.

■**Oper Status** – Indicates if the link is Up or Down.

■**Media Type** – Media type used.
(Options: 1000Base-T RJ-45 – Copper-Forced;
SFP – Copper-Forced, SFP-Forced, or SFP-Preferred-Auto;
XFP and 10GBase-T – SFP-Preferred-Auto;
Default: 1000Base-T RJ-45 – Copper-Forced,
SFP – SFP-Preferred-Auto,
XFP and 10GBase-T – SFP-Preferred-Auto)

■**Autonegotiation** – Shows if auto-negotiation is enabled or disabled.

■**Oper Speed Duplex** – Shows the current speed and duplex mode.

■**Oper Flow Control** – Shows if flow control is enabled or disabled.

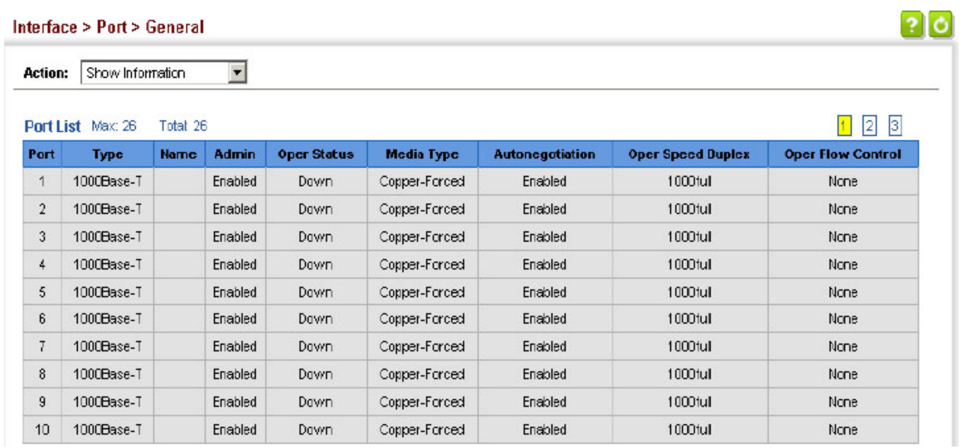
### WEB INTERFACE

To display port connection parameters:

**1.** Click Interface, Port, General.

**2.** Select Show Information from the Action List.

**Figure 3: Displaying Port Information**

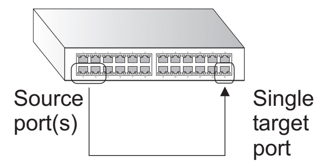



| Port | Type | Name | Admin | Oper Status | Media Type | Autonegotiation | Oper Speed Duplex | Oper Flow Control |
|---|---|---|---|---|---|---|---|---|
| 1 | 1000Base-T | | Enabled | Down | Copper-Forced | Enabled | 1000full | None |
| 2 | 1000Base-T | | Enabled | Down | Copper-Forced | Enabled | 1000full | None |
| 3 | 1000Base-T | | Enabled | Down | Copper-Forced | Enabled | 1000full | None |
| 4 | 1000Base-T | | Enabled | Down | Copper-Forced | Enabled | 1000full | None |
| 5 | 1000Base-T | | Enabled | Down | Copper-Forced | Enabled | 1000full | None |
| 6 | 1000Base-T | | Enabled | Down | Copper-Forced | Enabled | 1000full | None |
| 7 | 1000Base-T | | Enabled | Down | Copper-Forced | Enabled | 1000full | None |
| 8 | 1000Base-T | | Enabled | Down | Copper-Forced | Enabled | 1000full | None |
| 9 | 1000Base-T | | Enabled | Down | Copper-Forced | Enabled | 1000full | None |
| 10 | 1000Base-T | | Enabled | Down | Copper-Forced | Enabled | 1000full | None |

## Configuring Port Mirroring

Use the Interface > Port > Mirror page to mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

**Figure 4: Configuring Local Port Mirroring**




### CLI REFERENCES

■ "Local Port Mirroring Commands" on page 833

### COMMAND USAGE

■ Traffic can be mirrored from one or more source ports to one destination port on the same switch.

■ Monitor port speed should match or exceed source port speed, otherwise traffic may be dropped from the monitor port.

■ When mirroring port traffic, the target port must be included in the same VLAN as the source port when using MSTP (see "Spanning Tree Algorithm" on page 177).

### PARAMETERS

These parameters are displayed in the web interface:

■ **Source Port** – The port whose traffic will be monitored. (Range: 1-12/14/16/18) depending on the model

■ **Target Port** – The port that will mirror the traffic on the source port. (Range: 1-12/14/16/18) depending on the model

■ **Type** – Allows you to select which traffic to mirror to the target port, Rx (receive), Tx (transmit), or Both. (Default: Rx)

### WEB INTERFACE

To configure a local mirror session:

1. Click Interface, Port, Mirror.
2. Select Add from the Action List.
3. Specify the source port.
4. Specify the monitor port.
5. Specify the traffic type to be mirrored.
6. Click Apply.

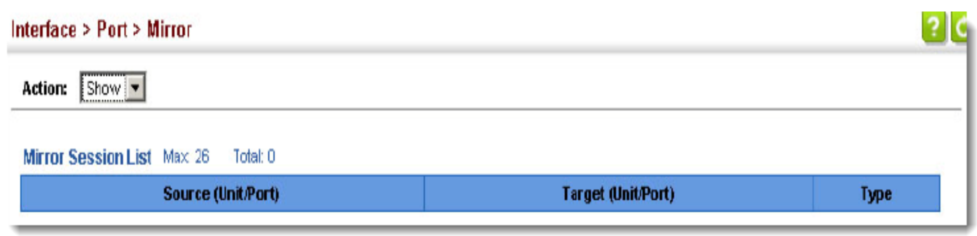
**Figure 5: Configuring Local Port Mirroring**


To display the configured mirror sessions:

1. Click Interface, Port, Mirror.

2. Select Show from the Action List.

**Figure 6: Displaying Local Port Mirror Sessions**




## Showing Port or Trunk Statistics

Use the Interface > Port/Trunk > Statistics or Chart page to display standard statistics on network traffic from the Interfaces Group and Ethernet-like MIBs, as well as a detailed breakdown of traffic based on the RMON MIB. Interfaces and Ethernet-like statistics display errors on the traffic passing through each port. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port. All values displayed have been accumulated since the last system reboot, and are shown as counts per second. Statistics are refreshed every 60 seconds by default.

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

### CLI REFERENCES

- "show interfaces counters" on page 815

### PARAMETERS

These parameters are displayed in the web interface:

**Table 1: Port Statistics**

| Parameter | Description |
|---|---|
| *Interface Statistics* | |
| Received Octets | The total number of octets received on the interface, including framing characters. |
| Transmitted Octets | The total number of octets transmitted out of the interface, including framing characters. |
| Received Errors | The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. |
| Transmitted Errors | The number of outbound packets that could not be transmitted because of errors. |
| Received Unicast Packets | The number of subnetwork-unicast packets delivered to a higher-layer protocol. |
| Transmitted Unicast Packets | The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent. |
| Received Discarded Packets | The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space. |
| Transmitted Discarded Packets | The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space. |
| Received Multicast Packets | The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer. |
| Transmitted Multicast Packets | The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. |
| Received Broadcast Packets | The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer. |
| Transmitted Broadcast Packets | The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent. |
| Received Unknown Packets | The number of packets received via the interface which were discarded because of an unknown or unsupported protocol. |
| *Etherlike Statistics* | |
| Single Collision Frames | The number of successfully transmitted frames for which transmission is inhibited by exactly one collision. |
| Multiple Collision Frames | A count of successfully transmitted frames for which transmission is inhibited by more than one collision. |
| Late Collisions | The number of times that a collision is detected later than 512 bit-times into the transmission of a packet. |
| Excessive Collisions | A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode. |
| Deferred Transmissions | A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy. |
| Frames Too Long | A count of frames received on a particular interface that exceed the maximum permitted frame size. |
| Alignment Errors | The number of alignment errors (missynchronized data packets). |

**Table 1: Port Statistics (Continued)**

| Parameter | Description |
|---|---|
| FCS Errors | A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error. |
| SQE Test Errors | A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. |
| Carrier Sense Errors | The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame. |
| Internal MAC Receive Errors | A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. |
| Internal MAC Transmit Errors | A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. |
| *RMON Statistics* | |
| Drop Events | The total number of events in which packets were dropped due to lack of resources. |
| Jabbers | The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error. |
| Fragments | The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error. |
| Collisions | The best estimate of the total number of collisions on this Ethernet segment. |
| Received Octets | Total number of octets of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization. |
| Received Packets | The total number of packets (bad, broadcast and multicast) received. |
| Broadcast Packets | The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets. |
| Multicast Packets | The total number of good packets received that were directed to this multicast address. |
| Undersize Packets | The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed. |
| Oversize Packets | The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. |
| 64 Bytes Packets | The total number of packets (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets). |
| 65-127 Byte Packets<br>128-255 Byte Packets<br>256-511 Byte Packets<br>512-1023 Byte Packets<br>1024-1518 Byte Packets<br>1519-1536 Byte Packets | The total number of packets (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets). |
| *Utilization Statistics* | |
| Input Octets per second | Number of octets entering this interface per second. |
| Input Packets per second | Number of packets entering this interface per second. |
| Input Utilization | The input utilization rate for this interface. |
| Output Octets per second | Number of octets leaving this interface per second. |

**Table 1: Port Statistics (Continued)**

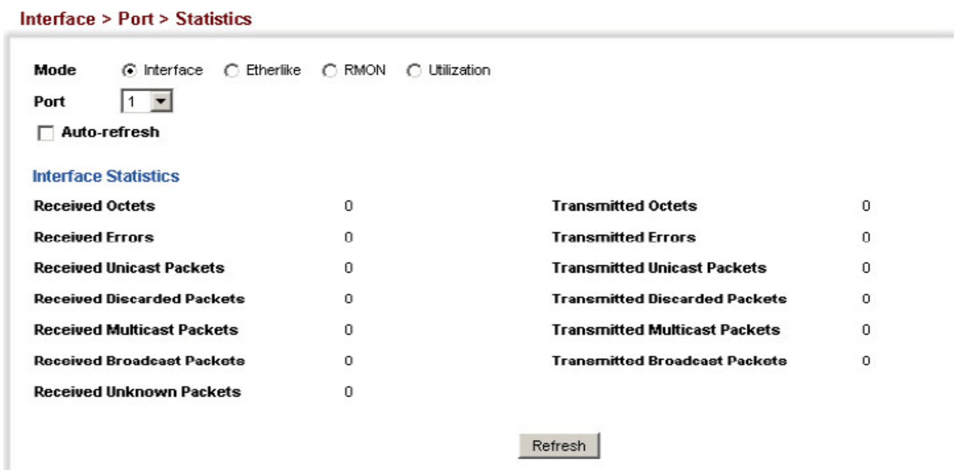
| Parameter | Description |
|---|---|
| Output Packets per second | Number of packets leaving this interface per second. |
| Output Utilization | The output utilization rate for this interface. |

### WEB INTERFACE

To show a list of port statistics:

1. Click Interface, Port, Statistics.
2. Select the statistics mode to display (Interface, Etherlike or RMON).
3. Select a port from the drop-down list.
4. Use the Refresh button at the bottom of the page if you need to update the screen.

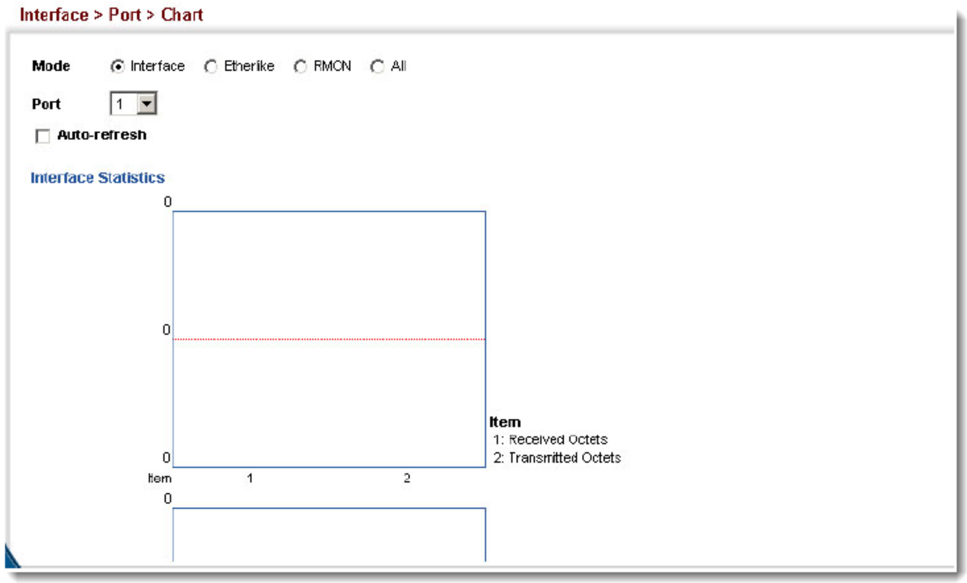
**Figure 7: Showing Port Statistics** (Table)




To show a chart of port statistics:

1. Click Interface, Port, Chart.
2. Select the statistics mode to display (Interface, Etherlike, RMON or All).
3. If Interface, Etherlike, RMON statistics mode is chosen, select a port from the drop-down list. If All (ports) statistics mode is chosen, select the statistics type to display.

**Figure 8: Showing Port Statistics** (Chart)




## Performing Cable Diagnostics

Use the Interface > Port > Cable Test page to test the cable attached to a port. The cable test will check for any cable faults (short, open, etc.). If a fault is found, the switch reports the length to the fault. Otherwise, it reports the cable length. It can be used to determine the quality of the cable, connectors, and terminations. Problems such as opens, shorts, and cable impedance mismatch can be diagnosed with this test.

### CLI REFERENCES

- "Interface Commands" on page 805

### COMMAND USAGE

- Cable diagnostics are performed using Digital Signal Processing (DSP) test methods. DSP analyses the cable by sending a pulsed signal into the cable, and then examining the reflection of that pulse.
- Cable diagnostics can only be performed on twisted-pair media.
- This cable test is only accurate for cables 7 - 140 meters long.
- The test takes approximately 5 seconds. The switch displays the results of the test immediately upon completion, including common cable failures, as well as the status and approximate length to a fault.
- Potential conditions which may be listed by the diagnostics include:
  - OK: Correctly terminated pair
  - Open: Open pair, no link partner
  - Short: Shorted pair
  - Not Supported: This message is displayed for any Gigabit Ethernet ports linked up at a speed lower than 1000 Mbps, or for any 10G Ethernet ports.

◆ Impedance mismatch: Terminating impedance is not in the reference range.

- Ports are linked down while running cable diagnostics.

### PARAMETERS

These parameters are displayed in the web interface:

- **Port** – Switch port identifier. (Range: 1-12/14/16/18) depending on the model
- **Test Result** – The results include common cable failures, as well as the status and approximate distance to a fault, or the approximate cable length if no fault is found.
- **Accuracy** – The accuracy of the reported length to a fault. (The accuracy displays “0” when no problem is found.)
- **Last Updated** – Shows the last time this port was tested.

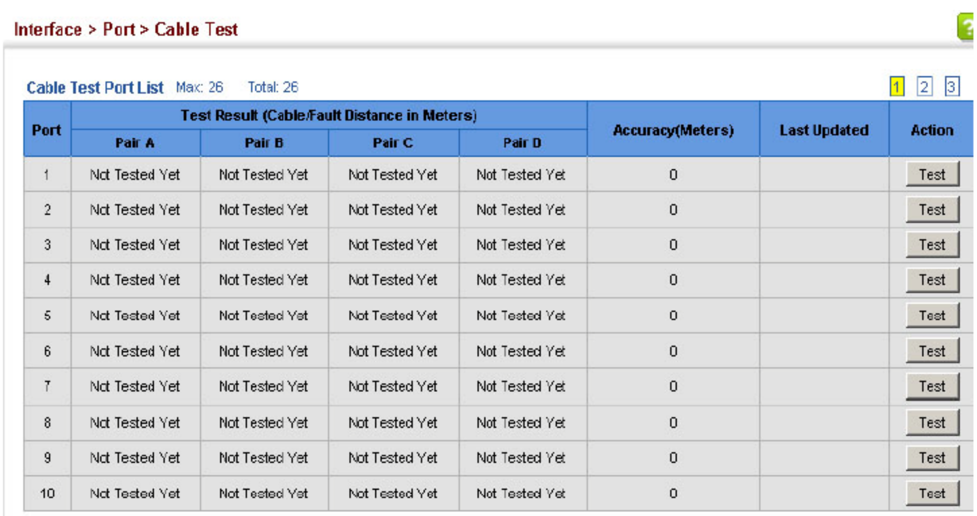
### WEB INTERFACE

To test the cable attached to a port:

1. Click Interface, Port, Cable Test.

2. Click Test for any port to start the cable test.

**Figure 9: Performing Cable Tests**


Interface > Port > Cable Test

Cable Test Port List Max: 26 Total: 26

1 2 3

| Port | Test Result (Cable/Fault Distance in Meters) | | | | Accuracy(Meters) | Last Updated | Action |
|---|---|---|---|---|---|---|---|
| | Pair A | Pair B | Pair C | Pair D | | | |
| 1 | Not Tested Yet | Not Tested Yet | Not Tested Yet | Not Tested Yet | 0 | | Test |
| 2 | Not Tested Yet | Not Tested Yet | Not Tested Yet | Not Tested Yet | 0 | | Test |
| 3 | Not Tested Yet | Not Tested Yet | Not Tested Yet | Not Tested Yet | 0 | | Test |
| 4 | Not Tested Yet | Not Tested Yet | Not Tested Yet | Not Tested Yet | 0 | | Test |
| 5 | Not Tested Yet | Not Tested Yet | Not Tested Yet | Not Tested Yet | 0 | | Test |
| 6 | Not Tested Yet | Not Tested Yet | Not Tested Yet | Not Tested Yet | 0 | | Test |
| 7 | Not Tested Yet | Not Tested Yet | Not Tested Yet | Not Tested Yet | 0 | | Test |
| 8 | Not Tested Yet | Not Tested Yet | Not Tested Yet | Not Tested Yet | 0 | | Test |
| 9 | Not Tested Yet | Not Tested Yet | Not Tested Yet | Not Tested Yet | 0 | | Test |
| 10 | Not Tested Yet | Not Tested Yet | Not Tested Yet | Not Tested Yet | 0 | | Test |

## TRUNK CONFIGURATION

This section describes how to configure static and dynamic trunks.

You can create multiple links between devices that work as one virtual, aggregate link. A port trunk offers a dramatic increase in bandwidth for network segments where bottlenecks exist, as well as providing a fault-tolerant link between two devices. You can create up to 13 trunks at a time on the EL326.

The switch supports both static trunking and dynamic Link Aggregation Control Protocol (LACP). Static trunks have to be manually configured at both ends of the link, and the switches must comply with the Cisco EtherChannel standard. On the other hand, LACP configured ports can automatically negotiate a trunked link with LACP-configured ports on another device. You can configure any number of ports on the switch as LACP, as long as they are not already configured as part of a static trunk. If ports on another device are also configured as LACP, the switch and the other device will negotiate a trunk link between them. If an LACP trunk consists of more than eight ports, all other ports will be placed in standby mode. Should one link in the trunk fail, one of the standby ports will automatically be activated to replace it.

### COMMAND USAGE

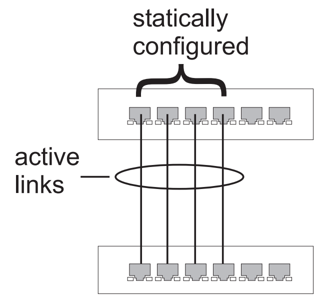
Besides balancing the load across each port in the trunk, the other ports provide redundancy by taking over the load if a port in the trunk fails. However, before making any physical connections between devices, use the web interface or CLI to specify the trunk on the devices at both ends. When using a port trunk, take note of the following points:

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- You can create up to 9 trunks on a MIL318, 8 trunks on a MIL316, 7 trunks on a MIL314 and 6 trunks on a MIL312, with up to 8 ports per trunk.
- The ports at both ends of a connection must be configured as trunk ports.
- When configuring static trunks on switches of different types, they must be compatible with the Cisco EtherChannel standard.
- The ports at both ends of a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- Any of the Gigabit ports on the front panel can be trunked together, including ports of different media types.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- STP, VLAN, and IGMP settings can only be made for the entire trunk.

### Configuring a Static Trunk

Use the Interface > Trunk > Static page to create a trunk, assign member ports, and configure the connection parameters.

**Figure 10: Configuring Static Trunks**




### CLI References

■"Link Aggregation Commands" on page 823
■"Interface Commands" on page 805

### Command Usage

- When configuring static trunks, you may not be able to link switches of different types, depending on the manufacturer's implementation. However, note that the static trunks on this switch are Cisco EtherChannel compatible.

- To avoid creating a loop in the network, be sure you add a static trunk via the configuration interface before connecting the ports, and also disconnect the ports before removing a static trunk via the configuration interface.

### Parameters

These parameters are displayed in the web interface:

- **Trunk ID** – Trunk identifier. (Range: 1-32)

- **Member** – The initial trunk member. Use the Add Member page to configure additional members.

  - **Unit** –1 Note: The MIL300 models only support unit 1.

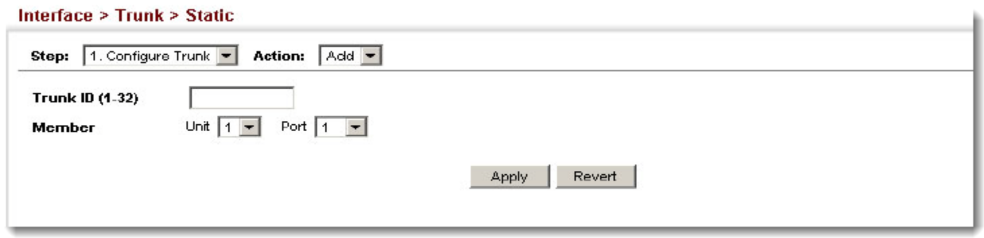
  - **Port** – Port identifier. (Range: 1-12/14/16/18) depending on the model

### Web Interface

To create a static trunk:

1. Click Interface, Trunk, Static.
2. Select Configure Trunk from the Step list.
3. Select Add from the Action list.
4. Enter a trunk identifier.
5. Set the unit and port for the initial trunk member.
6. Click Apply.

**Figure 11: Creating Static Trunks**




To add member ports to a static trunk:

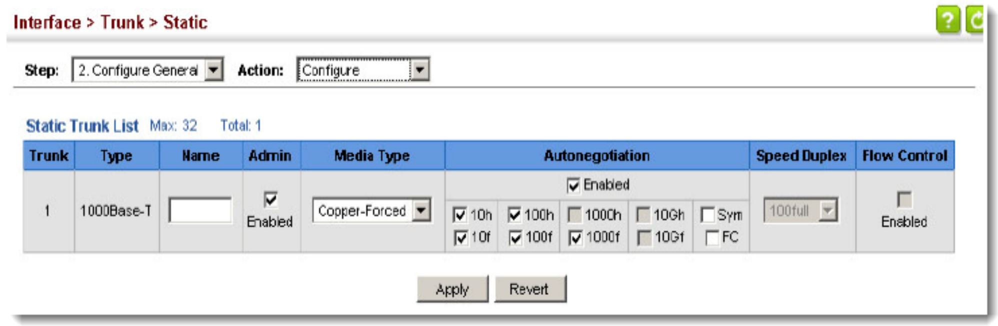
1. Click Interface, Trunk, Static.
2. Select Configure Trunk from the Step list.
3. Select Add Member from the Action list.
4. Select a trunk identifier.
5. Set the unit and port for an additional trunk member.
6. Click Apply.

**Figure 12: Adding Static Trunks Members**


To configure connection parameters for a static trunk:

1. Click Interface, Trunk, Static.
2. Select Configure General from the Step list.
3. Select Configure from the Action list.
4. Modify the required interface settings. (Refer to "Configuring by Port List" on page 107 for a description of the parameters.)
5. Click Apply.

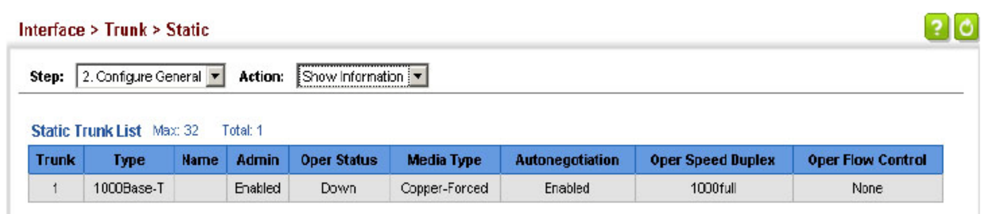
**Figure 13: Configuring Connection Parameters for a Static Trunk**




To display trunk connection parameters:

1. Click Interface, Trunk, Static.
2. Select Configure General from the Step list.
3. Select Show Information from the Action list.

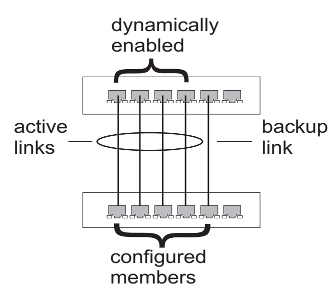
**Figure 14: Displaying Connection Parameters for Static Trunks**




## Configuring a Dynamic Trunk

Use the Interface > Trunk > Dynamic (Configure Aggregator) page to set the administrative key for an aggregation group, enable LACP on a port, and configure protocol parameters for local and partner ports.

**Figure 15: Configuring Dynamic Trunks**




### CLI REFERENCES

■ "Link Aggregation Commands" on page 823

### COMMAND USAGE

- To avoid creating a loop in the network, be sure you enable LACP before connecting the ports, and also disconnect the ports before disabling LACP.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- A trunk formed with another switch using LACP will automatically be assigned the next available trunk ID.
- If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.
- All ports on both ends of an LACP trunk must be configured for full duplex, and auto-negotiation.
- Ports are only allowed to join the same Link Aggregation Group (LAG) if (1) the LACP port system priority matches, (2) the LACP port admin key matches, and (3) the LAG admin key matches (if configured). However, if the LAG admin key is set, then the port admin key must be set to the same value for a port to be allowed to join that group.

---

If the LACP admin key is not set when a channel group is formed (i.e., it has a null value of 0), the operational value of this key is set to the same value as the port admin key used by the interfaces that joined the group (see the show lacp internal command described on page 829).

---

### PARAMETERS

These parameters are displayed in the web interface:

*Configure Aggregator*

- **Admin Key** – LACP administration key is used to identify a specific link aggregation group (LAG) during local LACP setup on the switch. (Range: 0-65535)

*Configure Aggregation Port - General*

- **Port** – Port identifier. (Range: 1-12/14/16/18) depending on the model
- **LACP Status** – Enables or disables LACP on a port.

*Configure Aggregation Port - Actor/Partner*

- **Port** – Port number. (Range: 1-12/14/16/18) depending on the model
- **Admin Key** – The LACP administration key must be set to the same value for ports that belong to the same LAG. (Range: 0-65535; Default: 1)

  By default, the Actor Admin Key is determined by port's link speed, and copied to Oper Key. The Partner Admin Key is assigned to zero, and the Oper Key is set based upon LACP PDUs received from the Partner.

- **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)

  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.

- **Port Priority** – If a link goes down, LACP port priority is used to select a backup link. (Range: 0-65535; Default: 32768)

---

Configuring LACP settings for a port only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with that port.

Configuring the port partner sets the remote side of an aggregate link; i.e., the ports on the attached device. The command attributes have the same meaning as those used for the port actor.

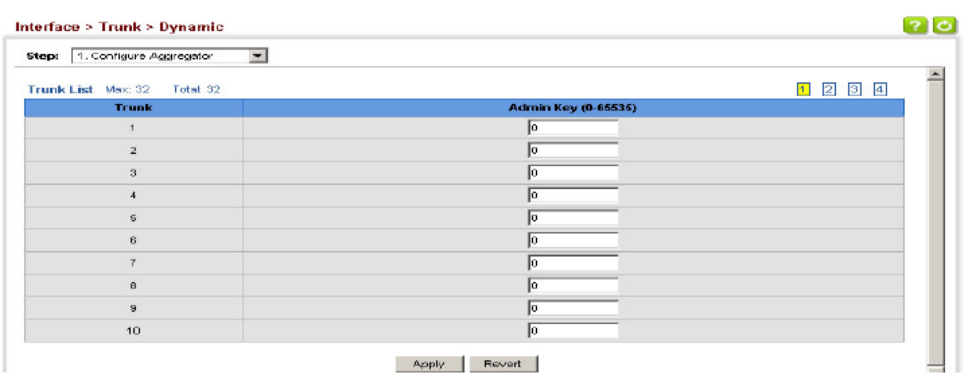
---

### WEB INTERFACE

To configure the admin key for a dynamic trunk:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Aggregator from the Step list.
3. Set the Admin Key for the required LACP group.
4. Click Apply.

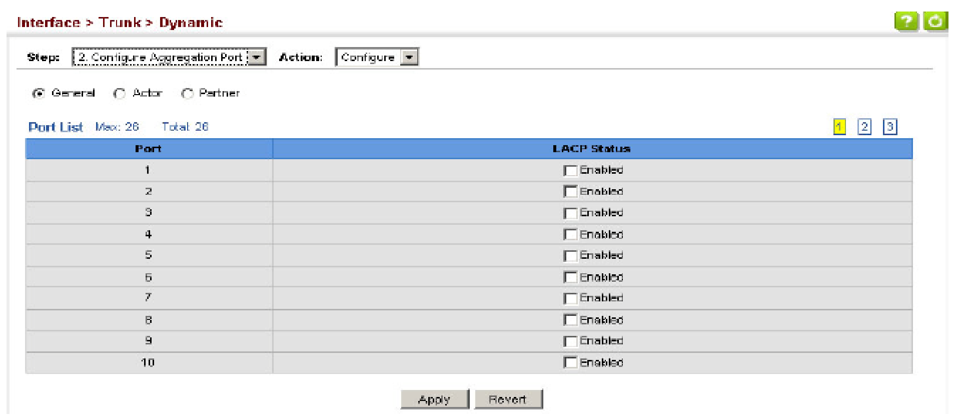
**Figure 16: Configuring the LACP Aggregator Admin Key**



To enable LACP for a port:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Aggregation Port from the Step list.
3. Select Configure from the Action list.
4. Click General.
5. Enable LACP on the required ports.
6. Click Apply.

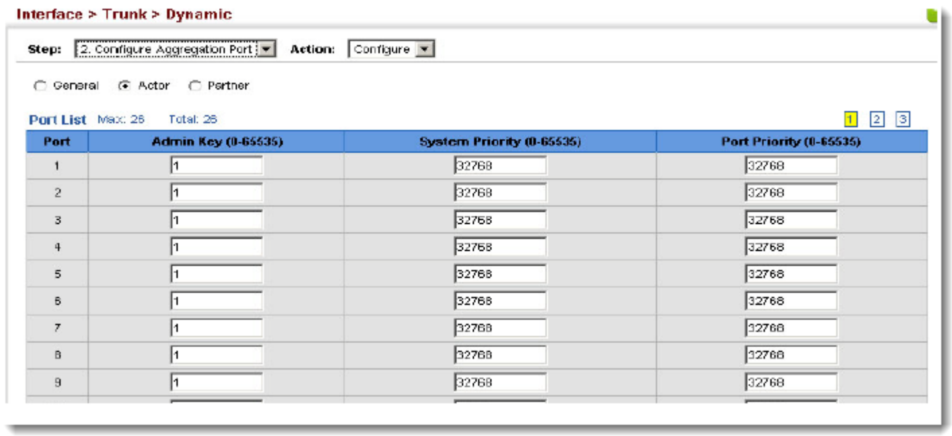
**Figure 17: Enabling LACP on a Port**




To configure LACP parameters for group members:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Aggregation Port from the Step list.
3. Select Configure from the Action list.
4. Click Actor or Partner.
5. Configure the required settings.
6. Click Apply.

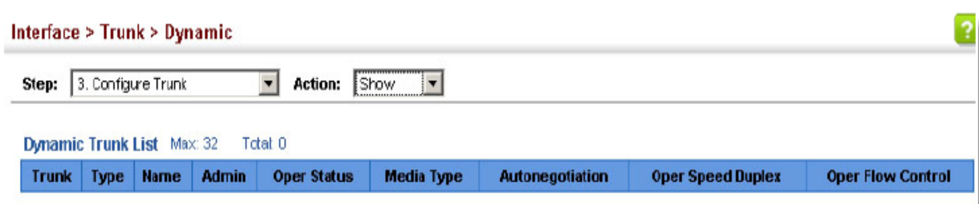
**Figure 18: Configuring LACP Parameters on a Port**




To show the active members of a dynamic trunk:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Trunk from the Step List.
3. Select Show Member from the Action List.
4. Select a Trunk.

**Figure 19: Showing Members of a Dynamic Trunk**




To configure connection parameters for a dynamic trunk:

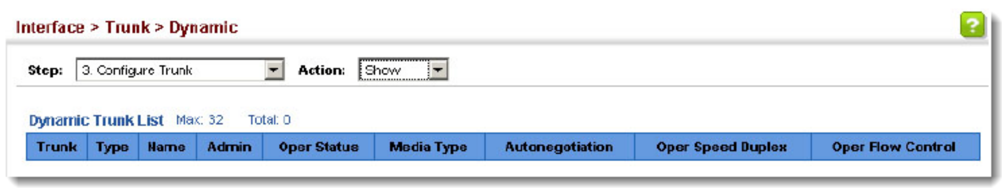
1. Click Interface, Trunk, Dynamic.
2. Select Configure Trunk from the Step List.
3. Select Configure from the Action List.
4. Modify the required interface settings. (See "Configuring by Port List" on page 107 for a description of the interface settings.)
5. Click Apply.

**Figure 20: Configuring Connection Settings for Dynamic Trunks**


To display connection parameters for a dynamic trunk:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Trunk from the Step List.
3. Select Show from the Action List.

**Figure 21: Displaying Connection Parameters for Dynamic Trunks**




## Displaying LACP Port Counters

Use the Interface > Trunk > Dynamic (Configure Aggregation Port - Show Information - Counters) page to display statistics for LACP protocol messages.

### CLI REFERENCES

■"show lacp" on page 829

### PARAMETERS

These parameters are displayed in the web interface:

**Table 2: LACP Port Counters**

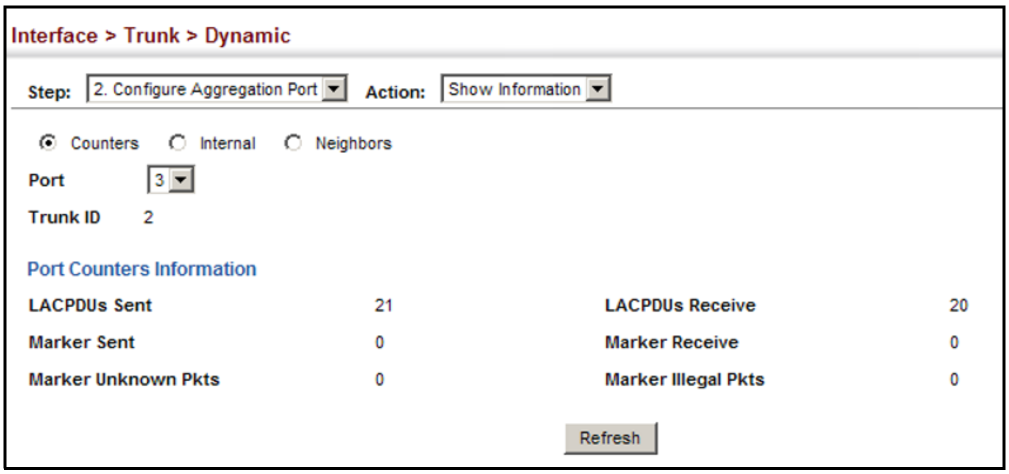
| Parameter | Description |
|---|---|
| LACPDUs Sent | Number of valid LACPDUs transmitted from this channel group. |
| LACPDUs Received | Number of valid LACPDUs received on this channel group. |
| Marker Sent | Number of valid Marker PDUs transmitted from this channel group. |
| Marker Received | Number of valid Marker PDUs received by this channel group. |
| Marker Unknown Pkts | Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type. |
| Marker Illegal Pkts | Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype. |

### WEB INTERFACE

To display LACP port counters:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Aggregation Port from the Step list.
3. Select Show Information from the Action list.
4. Click Counters.
5. Select a group member from the Port list.

**Figure 22: Displaying LACP Port Counters**




## Displaying LACP Settings and Status for the Local Side

Use the Interface > Trunk > Dynamic (Configure Aggregation Port - Show Information - Internal) page to display the configuration settings and operational state for the local side of a link aggregation.

### CLI REFERENCES

- "show lacp" on page 829

### PARAMETERS

These parameters are displayed in the web interface:

**Table 3: LACP Internal Configuration Information**

| Parameter | Description |
|---|---|
| LACP System Priority | LACP system priority assigned to this port channel. |
| LACP Port Priority | LACP port priority assigned to this interface within the channel group. |
| Admin Key | Current administrative value of the key for the aggregation port. |
| Oper Key | Current operational value of the key for the aggregation port. |
| LACPDUs Interval | Number of seconds before invalidating received LACPDU information. |

**Table 3: LACP Internal Configuration Information (Continued)**

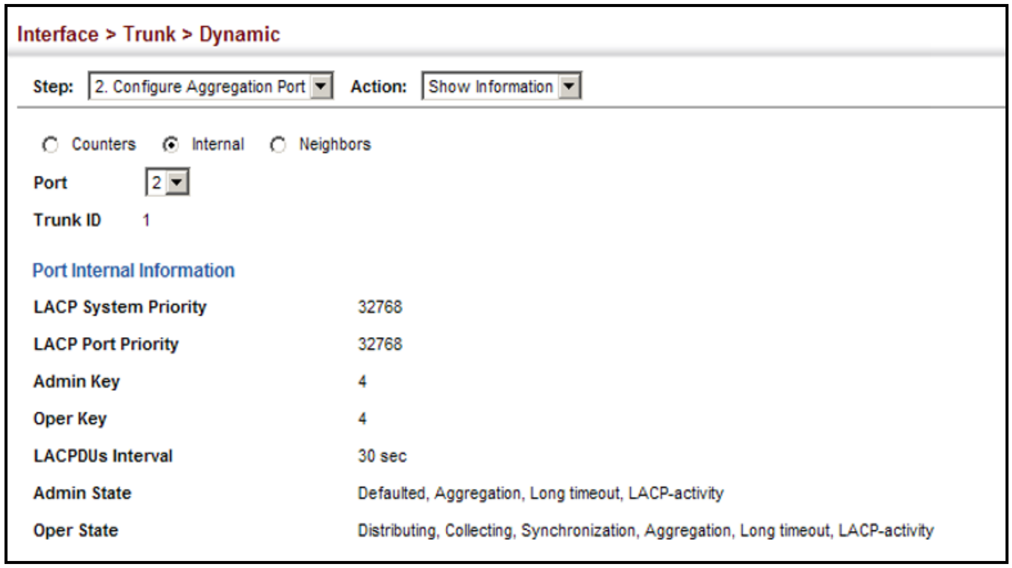
| Parameter | Description |
|---|---|
| Admin State, Oper State | Administrative or operational values of the actor's state parameters:<br>◆ Expired – The actor's receive machine is in the expired state;<br>◆ Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner.<br>◆ 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.<br>◆ 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.<br>◆ 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.<br>◆ Aggregation – The system considers this link to be aggregatable; i.e., a potential candidate for aggregation.<br>◆ Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate.<br>◆ LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active) |

### WEB INTERFACE

To display LACP settings and status for the local side:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Aggregation Port from the Step list.
3. Select Show Information from the Action list.
4. Click Internal.
5. Select a group member from the Port list.

**Figure 23: Displaying LACP Port Internal Information**




## Displaying LACP Settings and Status for the Remote Side

Use the Interface > Trunk > Dynamic (Configure Aggregation Port - Show Information - Neighbors) page to display the configuration settings and operational state for the remote side of a link aggregation.

### CLI REFERENCES

■ "show lacp" on page 829

### PARAMETERS

These parameters are displayed in the web interface:

**Table 4: LACP Internal Configuration Information**

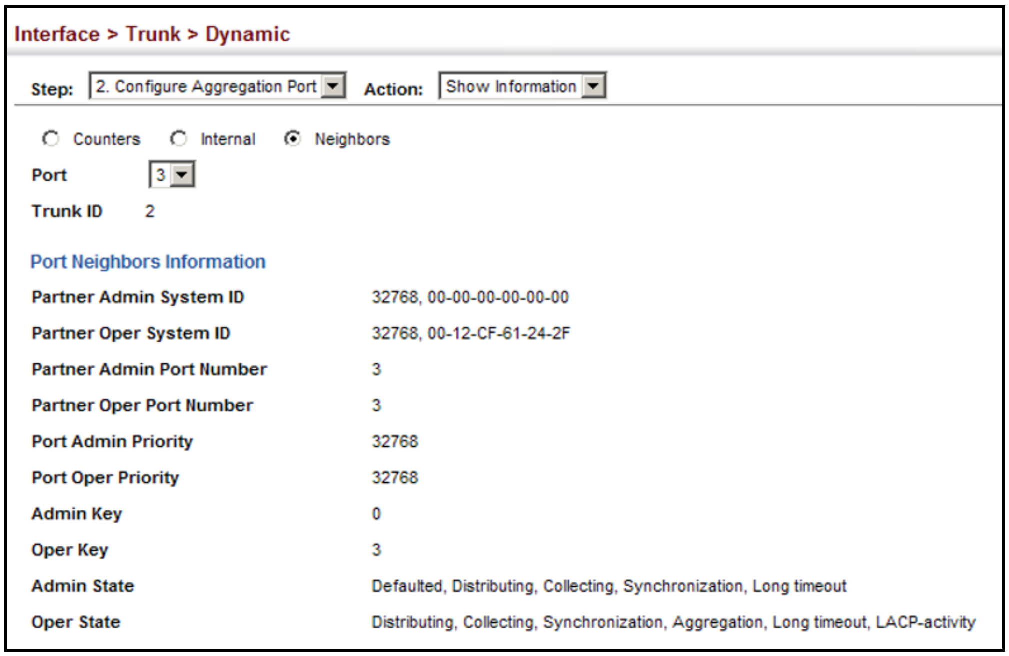
| Parameter | Description |
|---|---|
| Partner Admin System ID | LAG partner's system ID assigned by the user. |
| Partner Oper System ID | LAG partner's system ID assigned by the LACP protocol. |
| Partner Admin Port Number | Current administrative value of the port number for the protocol Partner. |
| Partner Oper Port Number | Operational port number assigned to this aggregation port by the port's protocol partner. |
| Port Admin Priority | Current administrative value of the port priority for the protocol partner. |
| Port Oper Priority | Priority value assigned to this aggregation port by the partner. |
| Admin Key | Current administrative value of the Key for the protocol partner. |
| Oper Key | Current operational value of the Key for the protocol partner. |
| Admin State | Administrative values of the partner's state parameters. (See preceding table.) |
| Oper State | Operational values of the partner's state parameters. (See preceding table.) |

**WEB INTERFACE**

To display LACP settings and status for the remote side:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Aggregation Port from the Step list.
3. Select Show Information from the Action list.
4. Click Neighbors.
5. Select a group member from the Port list.

**Figure 24: Displaying LACP Port Remote Information**




## SAMPLING TRAFFIC FLOWS

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

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

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

## Configuring sFlow Parameters

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

### CLI REFERENCES

- "Flow Sampling Commands" on page 685

### PARAMETERS

These parameters are displayed in the web interface:

- **Port** – Choose the port to configure. (Range: 1-12/14/16/18; Default: 1)
- **Status** – Enables sFlow on the selected port.
- **Receiver Owner**[1] – The name of the receiver. (Range: 1-256 characters; Default: None)
- **Receiver IP Address**[1] – IP address of the sFlow Collector.
- **Receiver Port**[1] – The UDP port on which the sFlow Collector is listening for sFlow streams. (Range: 0-65534; Default: 6343)
- **Timeout** – The time that the sFlow process will continuously send samples to the Collector before resetting all sFlow port parameters. (Range: 0-10000000 seconds, where 0 indicates no time out)

  The sFlow parameters affected by this command include the sampling interval, the receiver's name, address and UDP port, the time out, maximum header size, and maximum datagram size.
- **Max Header Size** – Maximum size of the sFlow datagram header. (Range: 64-256 bytes; Default: 128 bytes)
- **Max Datagram Size** – Maximum size of the sFlow datagram payload. (Range: 200-1500 bytes; Default: 1400 bytes)

1. Sampling must be disabled by setting the time out to 0 before these fields can be configured.

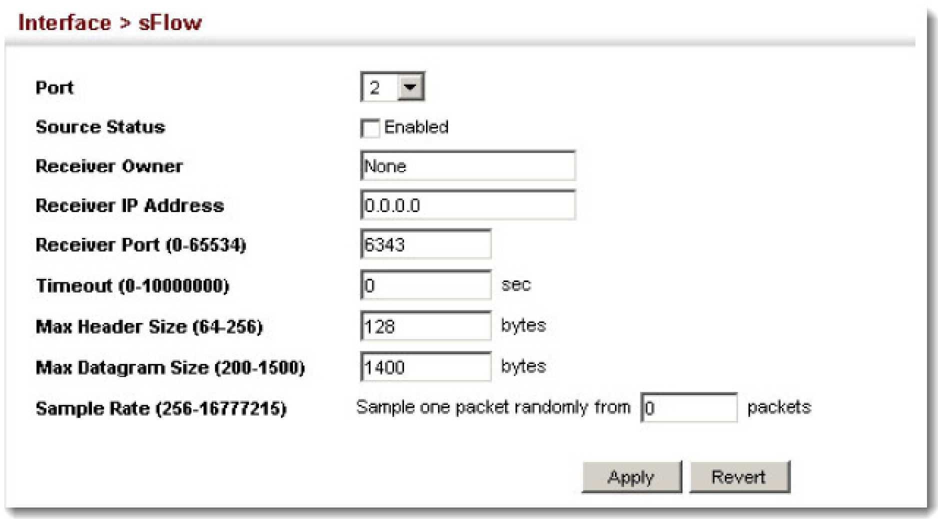
■**Sample Rate** – The number of packets out of which one sample will be taken. (Range: 256-16777215 packets, or 0 to disable sampling; Default: Disabled)

### WEB INTERFACE

To configure flow sampling:

1. Click Interface, sFlow.
2. Set the parameters for flow collector, the reset timeout, the payload, and the sampling rate.
3. Click Apply.

**Figure 25: Sampling Traffic Flows**




## TRAFFIC SEGMENTATION

If tighter security is required for passing traffic from different clients through downlink ports on the local network and over uplink ports to the service provider, port-based traffic segmentation can be used to isolate traffic between clients on different downlink ports. Data traffic on downlink ports is only forwarded to, and from, uplink ports.

### Enabling Traffic Segmentation

Use the Interface > Traffic Segmentation (Configure Global) page to enable traffic segmentation.

### CLI REFERENCES

■"Configuring Port-based Traffic Segmentation" on page 905

### PARAMETERS

These parameters are displayed in the web interface:

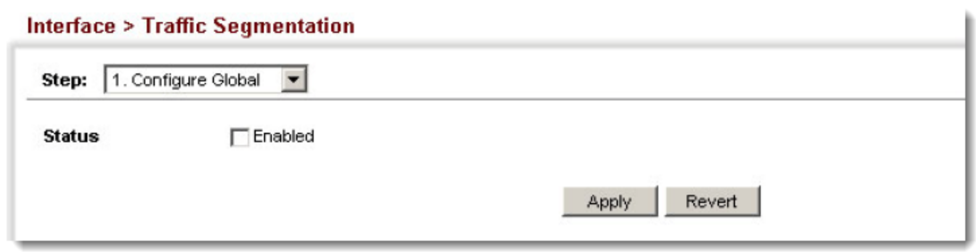
■**Status** – Enables port-based traffic segmentation. (Default: Disabled)

### WEB INTERFACE

To enable traffic segmentation:

1. Click Interface, Traffic Segmentation.
2. Select Configure Global from the Step list.
3. Mark the Enabled check box.
4. Click Apply.

**Figure 26: Enabling Traffic Segmentation**




## Configuring Uplink and Downlink Ports

Use the Interface > Traffic Segmentation (Configure Session) page to assign the downlink and uplink ports to use in the segmented group. Ports designated as downlink ports can not communicate with any other ports on the switch except for the uplink ports. Uplink ports can communicate with any other ports on the switch and with any designated downlink ports.

### CLI REFERENCES

- "Configuring Port-based Traffic Segmentation" on page 905

### PARAMETERS

These parameters are displayed in the web interface:

- **Interface** – Displays a list of ports or trunks.
- **Port** – Port Identifier. (Range: 1-12/14/16/18) depending on the model
- **Trunk** – Trunk Identifier. (Range: 1-32)
- **Direction** – Adds an interface to the segmented group by setting the direction to uplink or downlink. (Default: None)

### WEB INTERFACE

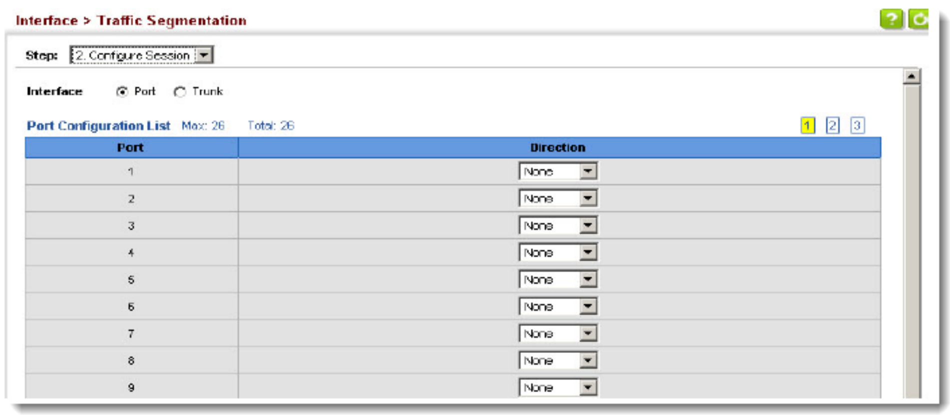
To configure the members of the traffic segmentation group:

1. Click Interface, Traffic Segmentation.
2. Select Configure Session from the Step list.
3. Click Port or Trunk to specify the interface type.

4. Select Uplink or Downlink in the Direction list to add a group member.

5. Click Apply.

**Figure 27: Configuring Members for Traffic Segmentation**




## VLAN TRUNKING

Use the Interface > VLAN Trunking page to allow unknown VLAN groups to pass through the specified interface.

### CLI REFERENCES

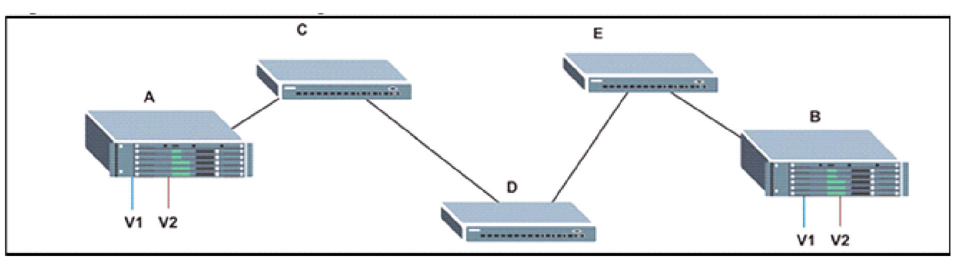
- "vlan-trunking" on page 897

### COMMAND USAGE

- Use this feature to configure a tunnel across one or more intermediate switches which pass traffic for VLAN groups to which they do not belong.

  The following figure shows VLANs 1 and 2 configured on switches A and B, with VLAN trunking being used to pass traffic for these VLAN groups across switches C, D and E.

  **Figure 28: Configuring VLAN Trunking**


  Without VLAN trunking, you would have to configure VLANs 1 and 2 on all intermediate switches – C, D and E; otherwise these switches would drop any frames with unknown VLAN group tags. However, by enabling VLAN trunking on the intermediate switch ports along the path connecting VLANs 1 and 2, you only need to create these VLAN groups in switches A and B. Switches C, D and E automatically allow frames with VLAN group tags 1 and 2 (groups that are unknown to those switches) to pass through their VLAN trunking ports.

- To prevent loops from forming in the spanning tree, all unknown VLANs will be bound to a single instance (either STP/RSTP or an MSTP instance, depending on the selected STA mode).

- If both VLAN trunking and ingress filtering are disabled on an interface, packets with unknown VLAN tags will still be allowed to enter this interface and will be flooded to all other ports where VLAN trunking is enabled. (In other words, VLAN trunking will still be effectively enabled for the unknown VLAN).

### PARAMETERS

These parameters are displayed in the web interface:

- **Interface** – Displays a list of ports or trunks.

- **Port** – Port Identifier. (Range: 1-12/14/16/18) depending on the model
- **Trunk** – Trunk Identifier. (Range: 1-32)

- **VLAN Trunking Status** – Enables VLAN trunking on the selected interface.

### WEB INTERFACE

To enable VLAN trunking on a port or trunk:

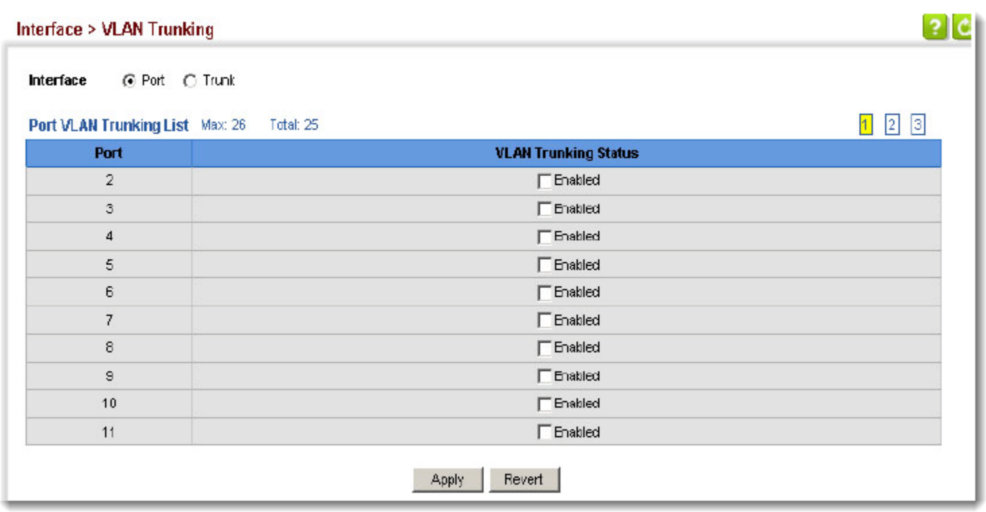
1. Click Interface, VLAN Trunking.

2. Click Port or Trunk to specify the interface type.

3. Enable VLAN trunking on any of the Gigibit ports or on a trunk containing Gigabit ports.

4. Click Apply.

**Figure 29: Configuring VLAN Trunking**



# 6 VLAN CONFIGURATION

This chapter includes the following topics:

- IEEE 802.1Q VLANs – Configures static and dynamic VLANs.
- Private VLANs – Configures private VLANs, using primary for unrestricted upstream access and community groups which are restricted to other local group members or to the ports in the associated primary group.
- IEEE 802.1Q Tunneling – Configures QinQ tunneling to maintain customer-specific VLAN and Layer 2 protocol configurations across a service provider network, even when different customers use the same internal VLAN IDs.
- Protocol VLANs – Configures VLAN groups based on specified protocols.
- IP Subnet VLANs – Maps untagged ingress frames to a specified VLAN if the source address is found in the IP subnet-to-VLAN mapping table.
- MAC-based VLANs – Maps untagged ingress frames to a specified VLAN if the source MAC address is found in the IP MAC address-to-VLAN mapping table.

## IEEE 802.1Q VLANS

In large networks, routers are used to isolate broadcast traffic for each subnet into separate domains. This switch provides a similar service at Layer 2 by using VLANs to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as video conferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

This switch supports the following VLAN features:

- Up to 4093 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**

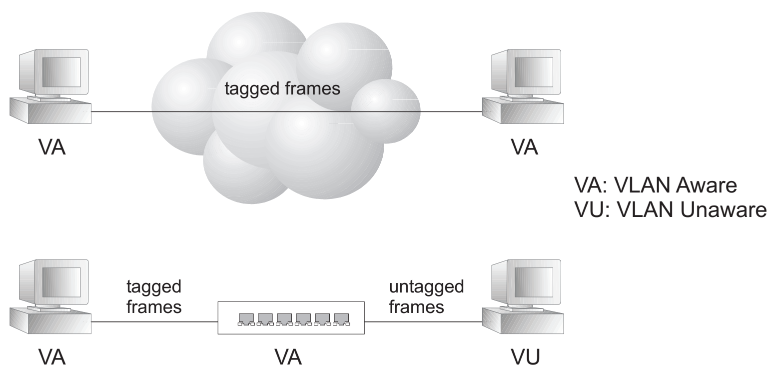
Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices 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.

---

**Figure 1: VLAN Compliant and VLAN Non-compliant Devices**




**VLAN Classification** – When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the default VLAN ID of the receiving port). But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

**Port Overlapping** – Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by enabled routing on this switch.

**Untagged VLANs** – Untagged (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 end station requests.

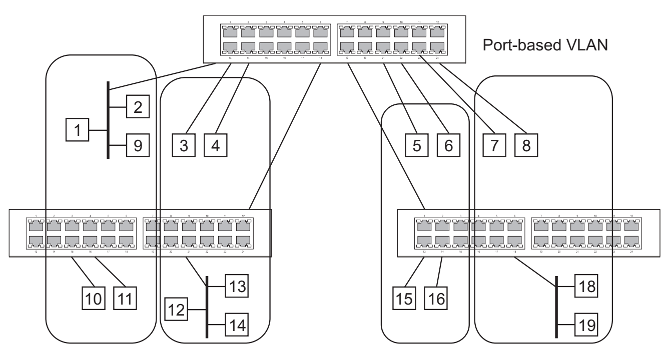
To implement GVRP in a network, first add the host devices to the required VLANs (using the operating system or other application software), so that these VLANs can be propagated onto the network. For both the edge switches attached directly to these hosts, and core switches in the network, enable GVRP on the links between these devices. You should also determine security boundaries in the network and disable GVRP on the boundary ports to prevent advertisements from being propagated, or forbid those ports from joining restricted VLANs.

---

If you have host devices that do not support GVRP, you should configure static or untagged VLANs for the switch ports connected to these devices (as described in "Adding Static Members to VLANs" on page 142). But you can still enable GVRP on these edge switches, as well as on the core switches in the network.

---

**Figure 2: Using GVRP**




### Forwarding Tagged/Untagged Frames

If you want to create a small port-based VLAN for devices attached directly to a single switch, you can assign ports to the same untagged VLAN. However, to participate in a VLAN group that crosses several switches, you should create a VLAN for that group and enable tagging on all ports.

Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is therefore capable of passing tagged or untagged frames. When forwarding a frame from this switch along a path that contains any VLAN-aware devices, the switch should include VLAN tags. When forwarding a frame from this switch along a path that does not contain any VLAN-aware devices (including the destination host), the switch must first strip off the VLAN tag before forwarding the frame. When the switch receives a tagged frame, it will pass this frame onto the VLAN(s) indicated by the frame tag. However, when this switch receives an untagged frame from a VLAN-unaware device, it first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID.

## Configuring VLAN Groups

Use the VLAN > Static (Add) page to create or remove VLAN groups. To propagate information about VLAN groups used on this switch to external network devices, you must specify a VLAN ID for each of these groups.

### CLI References

■"Editing VLAN Groups" on page 890

### Parameters

These parameters are displayed in the web interface:

*Add*

■**VLAN ID** – ID of VLAN or range of VLANs (1-4093).

■**Status** – Enables or disables the specified VLAN.

*Modify*

■**VLAN ID** – ID of configured VLAN (1-4093).

■**VLAN Name** – Name of the VLAN (1 to 32 characters).

■**Status** – Enables or disables the specified VLAN.

*Show*

■**VLAN ID** – ID of configured VLAN.

■**VLAN Name** – Name of the VLAN.

■**Status** – Operational status of configured VLAN.

### Web Interface

To create VLAN groups:

**1.** Click VLAN, Static.

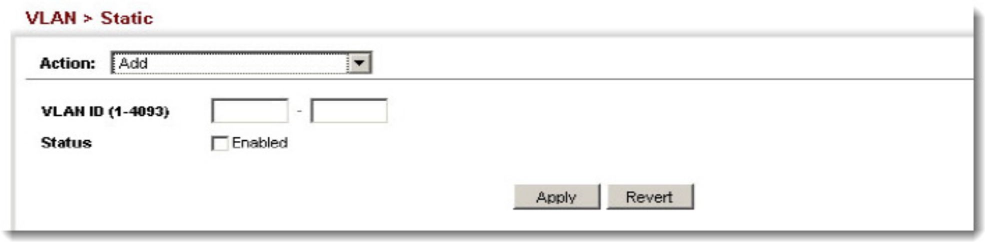
**2.** Select Add from the Action list.

**3.** Enter a VLAN ID or range of IDs.

**4.** Mark Enable to configure the VLAN as operational.

**5.** Click Apply.

**Figure 3: Creating Static VLANs**




To modify the configuration settings for VLAN groups:

**1.** Click VLAN, Static.

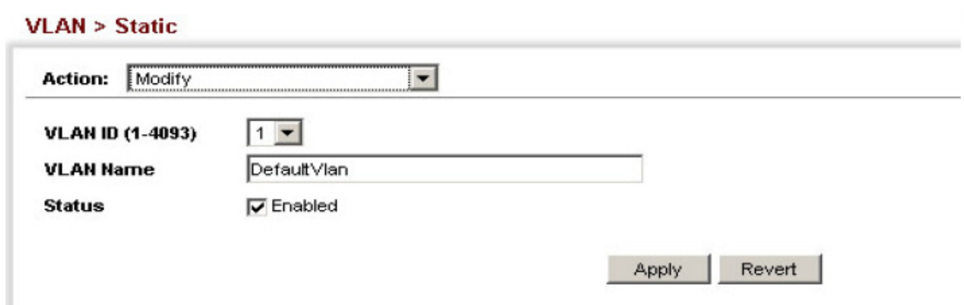
**2.** Select Modify from the Action list.

**3.** Select the identifier of a configured VLAN.

**4.** Modify the VLAN name or operational status as required.

**5.** Click Apply.

**Figure 4: Modifying Settings for Static VLANs**

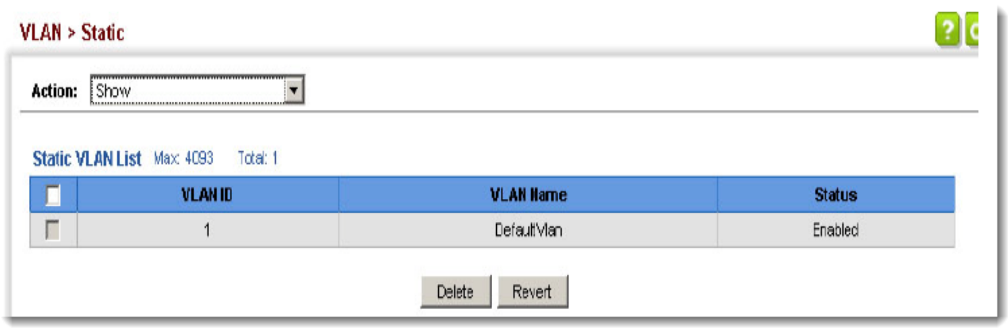


To show the configuration settings for VLAN groups:

1. Click VLAN, Static.

2. Select Show from the Action list.

**Figure 5: Showing Static VLANs**




## Adding Static Members to VLANs

Use the VLAN > Static page to configure port members for the selected VLAN index, interface, or a range of interfaces. Use the menus for editing port members to configure the VLAN behavior for specific interfaces, including the mode of operation (Hybrid or 1Q Trunk), the default VLAN identifier (PVID), accepted frame types, and ingress filtering. Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices, or untagged they are not connected to any VLAN-aware devices. Or configure a port as forbidden to prevent the switch from automatically adding it to a VLAN via the GVRP protocol.

### CLI References

■ "Configuring VLAN Interfaces" on page 892

■ "Displaying VLAN Information" on page 898

### Parameters

These parameters are displayed in the web interface:

*Edit Member by VLAN*

■ **VLAN** – ID of configured VLAN (1-4093).

■ **Interface** – Displays a list of ports or trunks.

■ **Port** – Port Identifier. (Range: 1-12/14/16/18) depending on the model

■ **Trunk** – Trunk Identifier. (Range: 1-32)

■ **Mode** – Indicates VLAN membership mode for an interface. (Default: Hybrid)

- ◆ **Hybrid** – Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.

- **1Q Trunk** – Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. Note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are also transmitted as tagged frames.

- **PVID** – 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, the PVID must be defined first, then the status of the VLAN can be configured as a tagged or untagged member.

- **Acceptable Frame Type** – Sets the interface to accept all frame types, including tagged or untagged frames, or only tagged frames. When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN. (Options: All, Tagged; Default: All)

- **Ingress Filtering** – Determines how to process frames tagged for VLANs for which the ingress port is not a member. (Default: Disabled)

  - Ingress filtering only affects tagged frames.
  - If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).
  - If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
  - Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STP. However, they do affect VLAN dependent BPDU frames, such as GMRP.

- **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 139.
  - **None**: Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.

VLAN 1 is the default untagged VLAN containing all ports on the switch, and membership type can only be modified by first assigning a port to another VLAN and then reassigning the default port VLAN ID.

*Edit Member by Interface*

All parameters are the same as those described under the preceding section for Edit Member by VLAN.

*Edit Member by Interface Range*

All parameters are the same as those described under the earlier section for Edit Member by VLAN, except for the items shown below.

- **Port Range** – Displays a list of ports. (Range: 1-12/14/16/18) depending on the model
- **Trunk Range** – Displays a list of ports. (Range: 1-32)

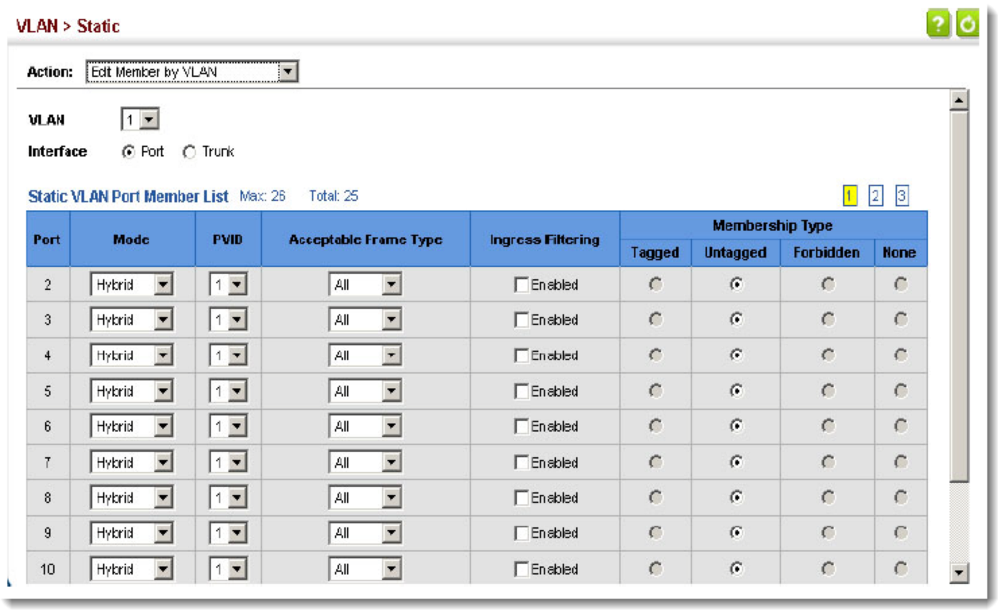
The PVID, acceptable frame type, and ingress filtering parameters for each interface within the specified range must be configured on either the Edit Member by VLAN or Edit Member by Interface page.

### Web Interface

To configure static members by the VLAN index:

1. Click VLAN, Static.
2. Select Edit Member by VLAN from the Step list.
3. Set the Interface type to display as Port or Trunk.
4. Modify the settings for any interface as required. Remember that Membership Type cannot be changed until an interface has been added to another VLAN and the PVID changed to anything other than 1.
5. Click Apply.

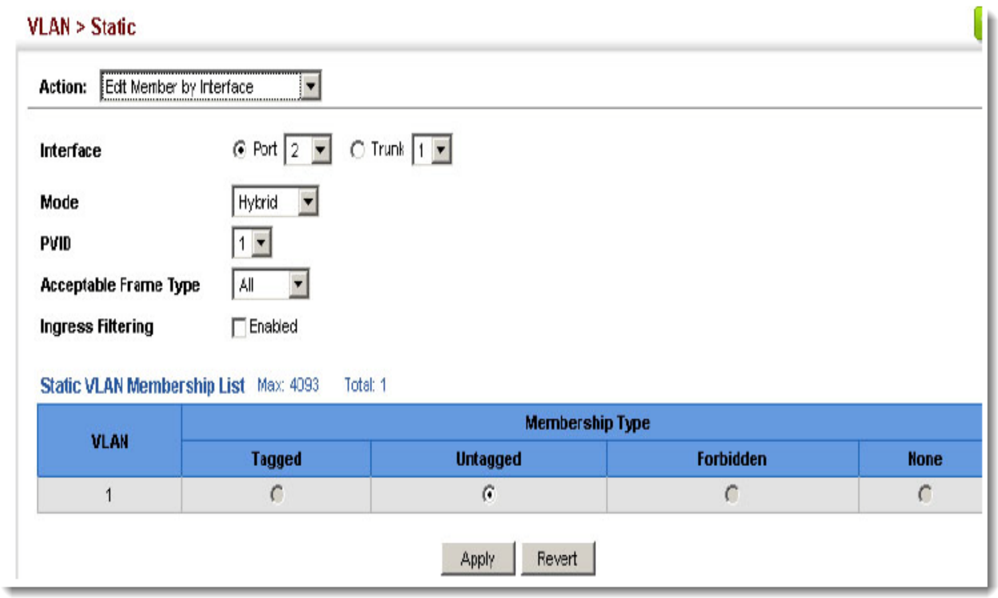
**Figure 6: Configuring Static Members by VLAN Index**




To configure static members by interface:

1. Click VLAN, Static.
2. Select Edit Member by Interface from the Step list.
3. Select a port or trunk configure.
4. Modify the settings for any interface as required.
5. Click Apply.

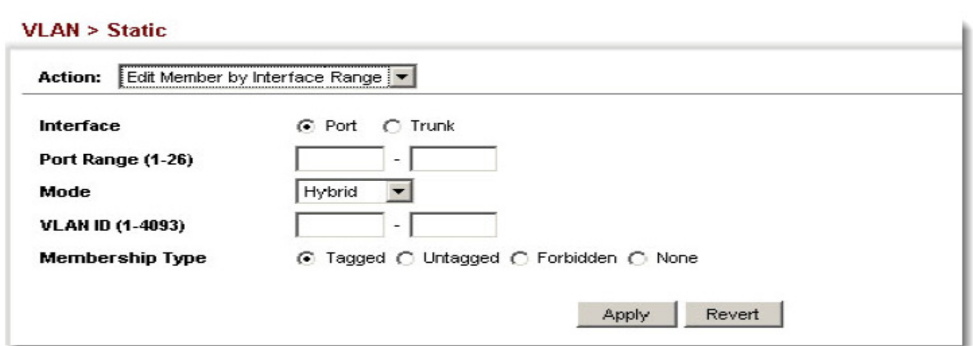
**Figure 7: Configuring Static VLAN Members by Interface**




To configure static members by interface range:

1. Click VLAN, Static.
2. Select Edit Member by Interface Range from the Step list.
3. Set the Interface type to display as Port or Trunk.
4. Enter an interface range.
5. Modify the VLAN parameters as required. Remember that the PVID, acceptable frame type, and ingress filtering parameters for each interface within the specified range must be configured on either the Edit Member by VLAN or Edit Member by Interface page.
6. Click Apply.

**Figure 8: Configuring Static VLAN Members by Interface Range**



## Configuring Dynamic VLAN Registration

Use the VLAN > Dynamic page to enable GVRP globally on the switch, or to enable GVRP and adjust the protocol timers per interface.

### CLI REFERENCES

■"GVRP and Bridge Extension Commands" on page 886
■"Configuring VLAN Interfaces" on page 892

### PARAMETERS

These parameters are displayed in the web interface:

*Configure General*

■**GVRP Status** – 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: Enabled)

*Configure Interface*

■**Interface** – Displays a list of ports or trunks.

■**Port** – Port Identifier. (Range: 1-12/14/16/18) depending on the model

■**Trunk** – Trunk Identifier. (Range: 1-32)

■**GVRP Status** – Enables/disables GVRP for the interface. GVRP must be globally enabled for the switch before this setting can take effect (using the Configure General page). When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. (Default: Disabled)

■**GVRP Timers –** Timer settings must follow this rule:
2 x (join timer) < leave timer < leaveAll timer

- ◆ **Join** – The interval between transmitting requests/queries to participate in a VLAN group. (Range: 20-1000 centiseconds; Default: 20)

- ◆ **Leave** – The interval a port waits before leaving a VLAN group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group. (Range: 60-3000 centiseconds; Default: 60)

- ◆ **LeaveAll** – The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group. (Range: 500-18000 centiseconds; Default: 1000)

*Show Dynamic VLAN – Show VLAN*

**VLAN ID** – Identifier of a VLAN this switch has joined through GVRP.

**VLAN Name –** Name of a VLAN this switch has joined through GVRP.

**Status** – Indicates if this VLAN is currently operational.
(Display Values: Enabled, Disabled)

*Show Dynamic VLAN – Show VLAN Member*

- **VLAN** – Identifier of a VLAN this switch has joined through GVRP.

- **Interface** – Displays a list of ports or trunks which have joined the selected VLAN through GVRP.

### Web Interface

To configure GVRP on the switch:

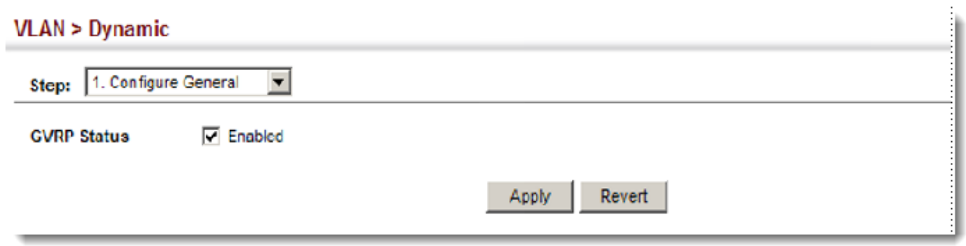
1. Click VLAN, Dynamic.

2. Select Configure General from the Step list.

3. Enable or disable GVRP.

4. Click Apply.

**Figure 9: Configuring Global Status of GVRP**




To configure GVRP status and timers on a port or trunk:

1. Click VLAN, Dynamic.

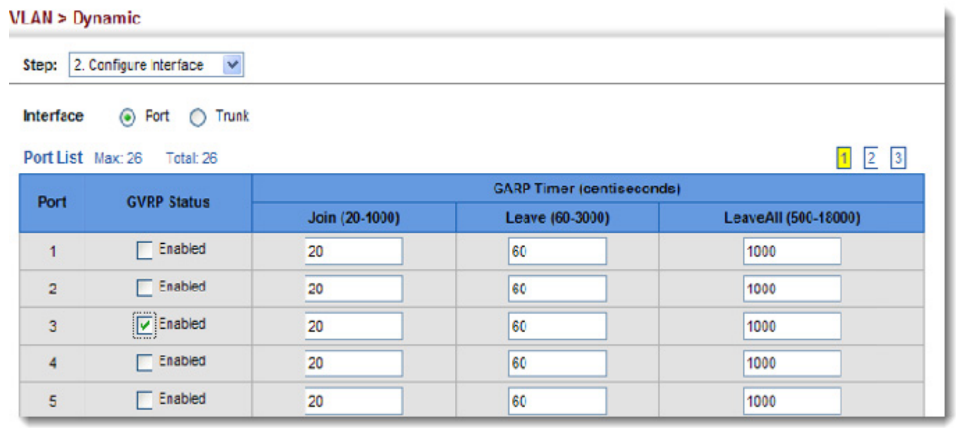
2. Select Configure Interface from the Step list.

3. Set the Interface type to display as Port or Trunk.

4. Modify the GVRP status or timers for any interface.

5. Click Apply.

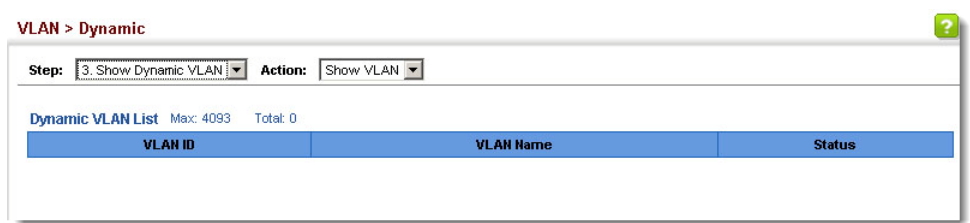
**Figure 10: Configuring GVRP for an Interface**




To show the dynamic VLAN joined by this switch:

1. Click VLAN, Dynamic.
2. Select Show Dynamic VLAN from the Step list.
3. Select Show VLAN from the Action list.

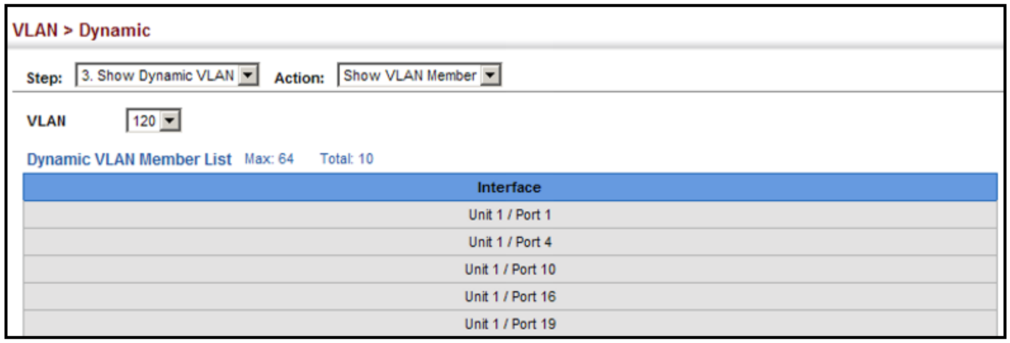
**Figure 11: Showing Dynamic VLANs Registered on the Switch**




To show the members of a dynamic VLAN:

1. Click VLAN, Dynamic.
2. Select Show Dynamic VLAN from the Step list.
3. Select Show VLAN Members from the Action list.

**Figure 12: Showing the Members of a Dynamic VLAN**




# Private VLANs

Private VLANs provide port-based security and isolation of local ports contained within different private VLAN groups. This switch supports two types of private VLANs – primary and community groups. A primary VLAN contains promiscuous ports that can communicate with all other ports in the associated private VLAN groups, while a community (or secondary) VLAN contains community ports that can only communicate with other hosts within the community VLAN and with any of the promiscuous ports in the associated primary VLAN. The promiscuous ports are designed to provide open access to an external network such as the Internet, while the community ports provide restricted access to local users.

Multiple primary VLANs can be configured on this switch, and multiple community VLANs can be associated with each primary VLAN. (Note that private VLANs and normal VLANs can exist simultaneously within the same switch.)

To configure primary/secondary associated groups, follow these steps:

1. Use the Configure VLAN (Add) page to designate one or more community VLANs, and the primary VLAN that will channel traffic outside of the VLAN groups.

2. Use the Configure VLAN (Add Community VLAN) page to map a community VLAN to the primary VLAN.

3. Use the Configure Interface page to set the port type to promiscuous (i.e., having access to all ports in the primary VLAN), or host (i.e., having access restricted to community VLAN members, and channeling all other traffic through promiscuous ports). Then assign any promiscuous ports to a primary VLAN and any host ports a community VLAN.

## Creating Private VLANs

Use the VLAN > Private (Configure VLAN - Add) page to create primary or community VLANs.

### CLI References

■"private-vlan" on page 908

**PARAMETERS**

These parameters are displayed in the web interface:

■**VLAN ID** – ID of configured VLAN (2-4093).

■**Type** – There are two types of private VLANs:

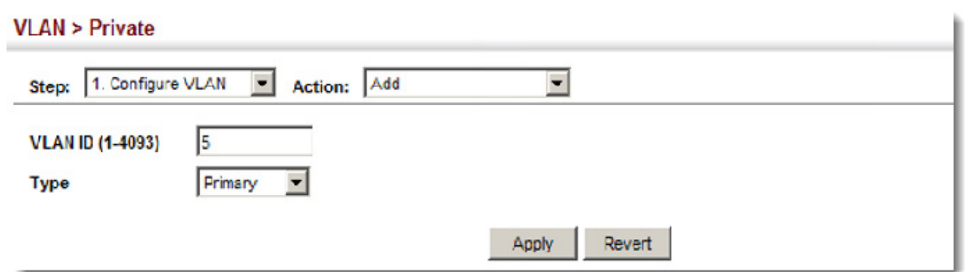
- **Primary** – Conveys traffic between promiscuous ports, and to community ports within secondary (or community) VLANs.
- **Community** - Conveys traffic between community ports, and to their promiscuous ports in the associated primary VLAN.

**WEB INTERFACE**

To configure private VLANs:

1. Click VLAN, Private.
2. Select Configure VLAN from the Step list.
3. Select Add from the Action list.
4. Enter the VLAN ID to assign to the private VLAN.
5. Select Primary or Community from the Type list
6. Click Apply.

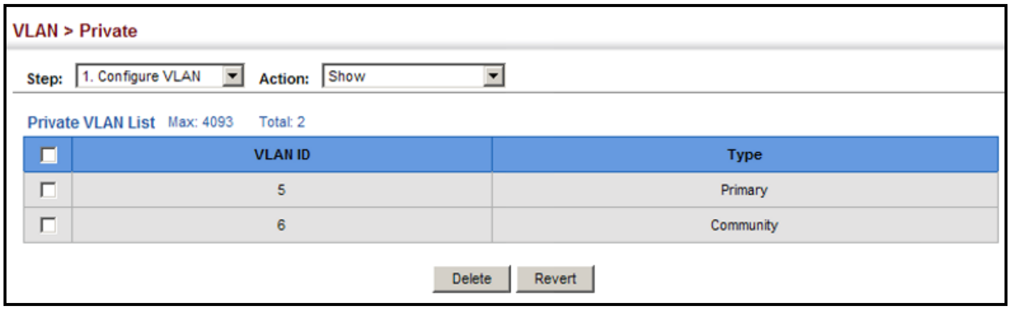
**Figure 13: Configuring Private VLANs**




To display a list of private VLANs:

1. Click VLAN, Private.
2. Select Configure VLAN from the Step list.
3. Select Show from the Action list.

**Figure 14: Showing Private VLANs**




All member ports must be removed from the VLAN before it can be deleted.

## Associating Private VLANs

Use the VLAN > Private (Configure VLAN - Add Community VLAN) page to associate each community VLAN with a primary VLAN.

### CLI REFERENCES

■ "private vlan association" on page 909

### PARAMETERS

These parameters are displayed in the web interface:

■ **Primary VLAN** – ID of primary VLAN (2-4093).

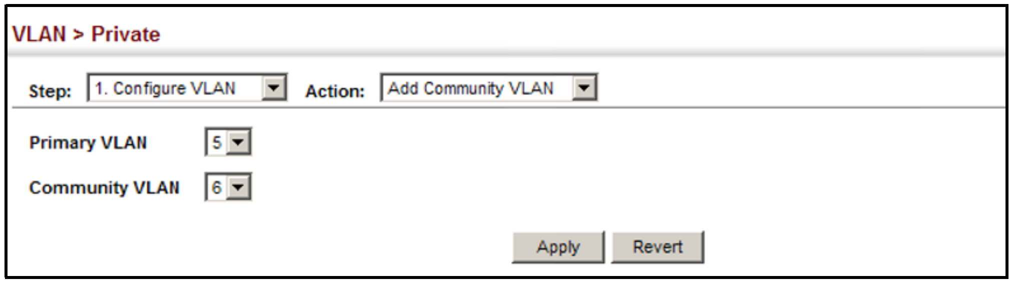
■ **Community VLAN** – VLAN associated with the selected primary VLAN.

### WEB INTERFACE

To associate a community VLAN with a primary VLAN:

1. Click VLAN, Private.
2. Select Configure VLAN from the Step list.
3. Select Add Community VLAN from the Action list.
4. Select an entry from the Primary VLAN list.
5. Select an entry from the Community VLAN list to associate it with the selected primary VLAN. Note that a community VLAN can only be associated with one primary VLAN.
6. Click Apply.

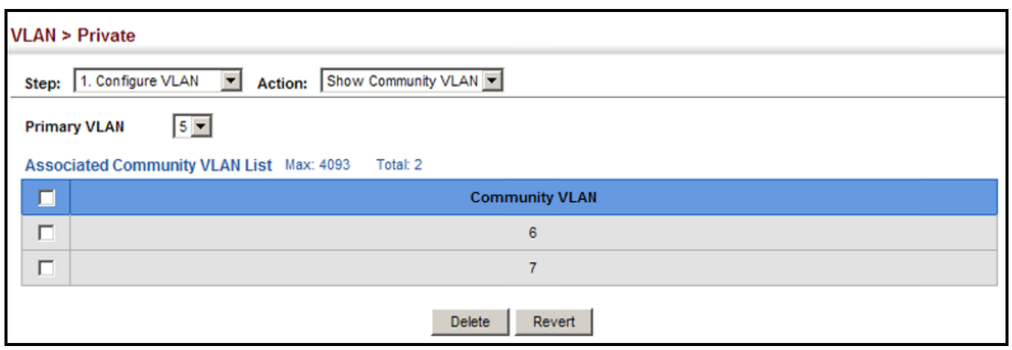
**Figure 15: Associating Private VLANs**




To show a list of community VLANs associated with a primary VLAN:

1. Click VLAN, Private.
2. Select Configure VLAN from the Step list.
3. Select Show Community VLAN from the Action list.
4. Select an entry from the Primary VLAN list.

**Figure 16: Showing Associated VLANs**




## Configuring Private VLAN Interfaces

Use the VLAN > Private (Configure Interface) page to set the private VLAN interface type, and assign the interfaces to a private VLAN.

### CLI References

- "switchport private-vlan mapping" on page 910
- "switchport private-vlan host-association" on page 910

### Parameters

These parameters are displayed in the web interface:

- **Interface** – Displays a list of ports or trunks.
- **Port** – Port Identifier. (Range: 1-12/14/16/18) depending on the model
- **Trunk** – Trunk Identifier. (Range: 1-32)
- **Port/Trunk Mode** – Sets the private VLAN port types.

- **Normal** – The port is not assigned to a private VLAN.
- **Host** – The port is a community port. A community port can communicate with other ports in its own community VLAN and with designated promiscuous port(s).
- **Promiscuous** – A promiscuous port can communicate with all interfaces within a private VLAN.

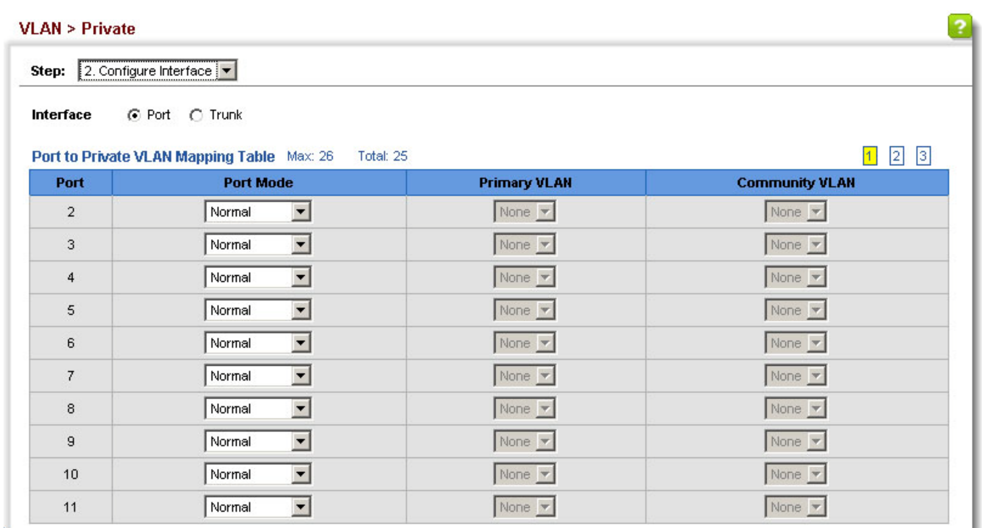
- **Primary VLAN** – Conveys traffic between promiscuous ports, and between promiscuous ports and community ports within the associated secondary VLANs. If Port Mode is “Promiscuous,” then specify the associated primary VLAN.
- **Community VLAN** – A community VLAN conveys traffic between community ports, and from community ports to their designated promiscuous ports. Set Port Mode to “Host,” and then specify the associated Community VLAN.

### Web Interface

To configure a private VLAN port or trunk:

1. Click VLAN, Private.
2. Select Configure Interface from the Step list.
3. Set the Interface type to display as Port or Trunk.
4. Set the Port Mode to Promiscuous.
5. For an interface set the Promiscuous mode, select an entry from the Primary VLAN list.
6. For an interface set the Host mode, select an entry from the Community VLAN list.
7. Click Apply.

**Figure 17: Configuring Interfaces for Private VLANs**



# IEEE 802.1Q TUNNELING

IEEE 802.1Q Tunneling (QinQ) is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting Service Provider VLAN (SPVLAN) tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4096.

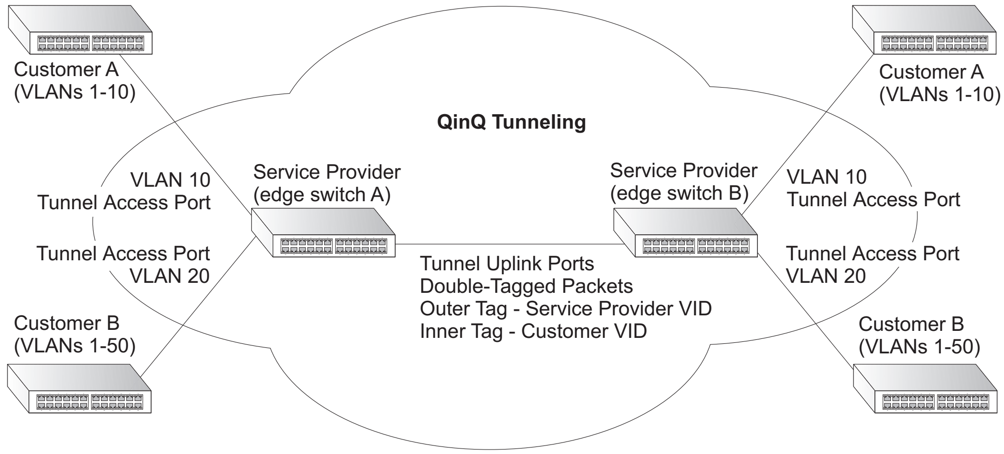
QinQ tunneling uses a single Service Provider VLAN (SPVLAN) for customers who have multiple VLANs. Customer VLAN IDs are preserved and traffic from different customers is segregated within the service provider's network even when they use the same customer-specific VLAN IDs. QinQ tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy, preserving the customer's original tagged packets, and adding SPVLAN tags to each frame (also called double tagging).

A port configured to support QinQ tunneling must be set to tunnel port mode. The Service Provider VLAN (SPVLAN) ID for the specific customer must be assigned to the QinQ tunnel access port on the edge switch where the customer traffic enters the service provider's network. Each customer requires a separate SPVLAN, but this VLAN supports all of the customer's internal VLANs. The QinQ tunnel uplink port that passes traffic from the edge switch into the service provider's metro network must also be added to this SPVLAN. The uplink port can be added to multiple SPVLANs to carry inbound traffic for different customers onto the service provider's network.

When a double-tagged packet enters another trunk port in an intermediate or core switch in the service provider's network, the outer tag is stripped for packet processing. When the packet exits another trunk port on the same core switch, the same SPVLAN tag is again added to the packet.

When a packet enters the trunk port on the service provider's egress switch, the outer tag is again stripped for packet processing. However, the SPVLAN tag is not added when it is sent out the tunnel access port on the edge switch into the customer's network. The packet is sent as a normal IEEE 802.1Q-tagged frame, preserving the original VLAN numbers used in the customer's network.

**Figure 18: QinQ Operational Concept**




*Layer 2 Flow for Packets Coming into a Tunnel Access Port*

A QinQ tunnel port may receive either tagged or untagged packets. No matter how many tags the incoming packet has, it is treated as tagged packet.

The ingress process does source and destination lookups. If both lookups are successful, the ingress process writes the packet to memory. Then the egress process transmits the packet. Packets entering a QinQ tunnel port are processed in the following manner:

1. New SPVLAN tags are added to all incoming packets, no matter how many tags they already have. The ingress process constructs and inserts the outer tag (SPVLAN) into the packet based on the default VLAN ID and Tag Protocol Identifier (TPID, that is, the ether-type of the tag). This outer tag is used for learning and switching packets. The priority of the inner tag is copied to the outer tag if it is a tagged or priority tagged packet.

2. After successful source and destination lookup, the ingress process sends the packet to the switching process with two tags. If the incoming packet is untagged, the outer tag is an SPVLAN tag, and the inner tag is a dummy tag (8100 0000). If the incoming packet is tagged, the outer tag is an SPVLAN tag, and the inner tag is a CVLAN tag.

3. After packet classification through the switching process, the packet is written to memory with one tag (an outer tag) or with two tags (both an outer tag and inner tag).

4. The switch sends the packet to the proper egress port.

5. If the egress port is an untagged member of the SPVLAN, the outer tag will be stripped. If it is a tagged member, the outgoing packets will have two tags.

*Layer 2 Flow for Packets Coming into a Tunnel Uplink Port*

An uplink port receives one of the following packets:

■Untagged

■One tag (CVLAN or SPVLAN)

■Double tag (CVLAN + SPVLAN)

The ingress process does source and destination lookups. If both lookups are successful, the ingress process writes the packet to memory. Then the egress process transmits the packet. Packets entering a QinQ uplink port are processed in the following manner:

1. If incoming packets are untagged, the PVID VLAN native tag is added.
2. If the ether-type of an incoming packet (single or double tagged) is not equal to the TPID of the uplink port, the VLAN tag is determined to be a Customer VLAN (CVLAN) tag. The uplink port's PVID VLAN native tag is added to the packet. This outer tag is used for learning and switching packets within the service provider's network. The TPID must be configured on a per port basis, and the verification cannot be disabled.
3. If the ether-type of an incoming packet (single or double tagged) is equal to the TPID of the uplink port, no new VLAN tag is added. If the uplink port is not the member of the outer VLAN of the incoming packets, the packet will be dropped when ingress filtering is enabled. If ingress filtering is not enabled, the packet will still be forwarded. If the VLAN is not listed in the VLAN table, the packet will be dropped.
4. After successful source and destination lookups, the packet is double tagged. The switch uses the TPID of 0x8100 to indicate that an incoming packet is double-tagged. If the outer tag of an incoming double-tagged packet is equal to the port TPID and the inner tag is 0x8100, it is treated as a double-tagged packet. If a single-tagged packet has 0x8100 as its TPID, and port TPID is not 0x8100, a new VLAN tag is added and it is also treated as double-tagged packet.
5. If the destination address lookup fails, the packet is sent to all member ports of the outer tag's VLAN.
6. After packet classification, the packet is written to memory for processing as a single-tagged or double-tagged packet.
7. The switch sends the packet to the proper egress port.
8. If the egress port is an untagged member of the SPVLAN, the outer tag will be stripped. If it is a tagged member, the outgoing packet will have two tags.

*Configuration Limitations for QinQ*

■The native VLAN of uplink ports should not be used as the SPVLAN. If the SPVLAN is the uplink port's native VLAN, the uplink port must be an untagged member of the SPVLAN. Then the outer SPVLAN tag will be stripped when the packets are sent out. Another reason is that it causes non-customer packets to be forwarded to the SPVLAN.

■Static trunk port groups are compatible with QinQ tunnel ports as long as the QinQ configuration is consistent within a trunk port group.

- The native VLAN (VLAN 1) is not normally added to transmitted frames. Avoid using VLAN 1 as an SPVLAN tag for customer traffic to reduce the risk of misconfiguration. Instead, use VLAN 1 as a management VLAN instead of a data VLAN in the service provider network.
- There are some inherent incompatibilities between Layer 2 and Layer 3 switching:
  - Tunnel ports do not support IP Access Control Lists.
  - Layer 3 Quality of Service (QoS) and other QoS features containing Layer 3 information are not supported on tunnel ports.
  - Spanning tree bridge protocol data unit (BPDU) filtering is automatically disabled on a tunnel port.

*General Configuration Guidelines for QinQ*

1. Enable Tunnel Status, and set the Tag Protocol Identifier (TPID) value of the tunnel access port (in the Ethernet Type field. This step is required if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The default ethertype value is 0x8100. (See "Enabling QinQ Tunneling on the Switch" on page 158.)
2. Create a Service Provider VLAN, also referred to as an SPVLAN (see "Configuring VLAN Groups" on page 140).
3. Configure the QinQ tunnel access port to Tunnel mode (see "Adding an Interface to a QinQ Tunnel" on page 159).
4. Configure the QinQ tunnel access port to join the SPVLAN as an untagged member (see "Adding Static Members to VLANs" on page 142).
5. Configure the SPVLAN ID as the native VID on the QinQ tunnel access port (see "Adding Static Members to VLANs" on page 142).
6. Configure the QinQ tunnel uplink port to Tunnel Uplink mode (see "Adding an Interface to a QinQ Tunnel" on page 159).
7. Configure the QinQ tunnel uplink port to join the SPVLAN as a tagged member (see "Adding Static Members to VLANs" on page 142).

## Enabling QinQ Tunneling on the Switch

Use the VLAN > Tunnel (Configure Global) page to configure the switch to operate in IEEE 802.1Q (QinQ) tunneling mode, which is used for passing Layer 2 traffic across a service provider's metropolitan area network. You can also globally set the Tag Protocol Identifier (TPID) value of the tunnel port if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames.

**CLI References**

- "Configuring IEEE 802.1Q Tunneling" on page 899

### PARAMETERS

These parameters are displayed in the web interface:

- **Tunnel Status** – Sets the switch to QinQ mode. (Default: Disabled)

- **Ethernet Type** – The Tag Protocol Identifier (TPID) specifies the ethertype of incoming packets on a tunnel port. (Range: hexadecimal 0800-FFFF; Default: 8100)

  Use this field to set a custom 802.1Q ethertype value. This feature allows the switch to interoperate with third-party switches that do not use the standard 0x8100 ethertype to identify 802.1Q-tagged frames. For example, if 0x1234 is set as the custom 802.1Q ethertype on a trunk port, incoming frames containing that ethertype are assigned to the VLAN contained in the tag following the ethertype field, as they would be with a standard 802.1Q trunk. Frames arriving on the port containing any other ethertype are looked upon as untagged frames, and assigned to the native VLAN of that port.

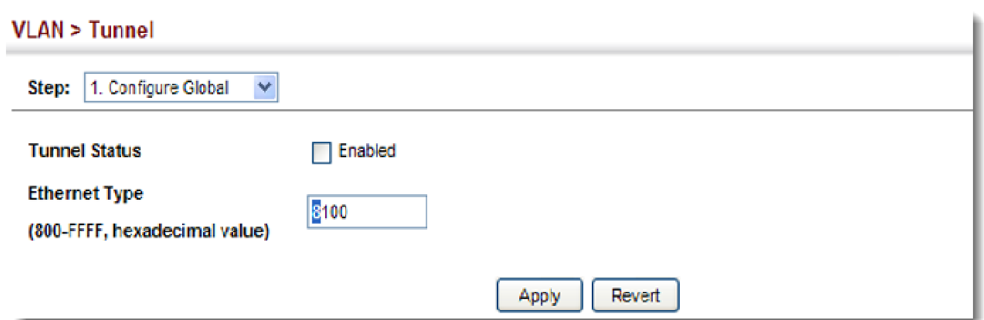
  All ports on the switch will be set to the same ethertype.

### WEB INTERFACE

To enable QinQ Tunneling on the switch:

1. Click VLAN, Tunnel.
2. Select Configure Global from the Step list.
3. Enable Tunnel Status, and specify the TPID if a client attached to a tunnel port is using a non-standard ethertype to identify 802.1Q tagged frames.
4. Click Apply.

**Figure 19: Enabling QinQ Tunneling**




## Adding an Interface to a QinQ Tunnel

Follow the guidelines in the preceding section to set up a QinQ tunnel on the switch. Then use the VLAN > Tunnel (Configure Interface) page to set the tunnel mode for any participating interface.

### CLI REFERENCES

- "Configuring IEEE 802.1Q Tunneling" on page 899

### Command Usage

- Use the Configure Global page to set the switch to QinQ mode before configuring a tunnel port or tunnel uplink port (see "Enabling QinQ Tunneling on the Switch" on page 158). Also set the Tag Protocol Identifier (TPID) value of the tunnel port if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames.

- Then use the Configure Interface page to set the access interface on the edge switch to Tunnel mode, and set the uplink interface on the switch attached to the service provider network to Tunnel Uplink mode.

### Parameters

These parameters are displayed in the web interface:

- **Interface** – Displays a list of ports or trunks.

- **Port** – Port Identifier. (Range: 1-12/14/16/18) depending on the model

- **Trunk** – Trunk Identifier. (Range: 1-32)

- **Mode** – Sets the VLAN membership mode of the port.
  - **None** – The port operates in its normal VLAN mode. (This is the default.)
  - **Tunnel** – Configures QinQ tunneling for a client access port to segregate and preserve customer VLAN IDs for traffic crossing the service provider network.
  - **Tunnel Uplink** – Configures QinQ tunneling for an uplink port to another device within the service provider network.

### Web Interface

To add an interface to a QinQ tunnel:

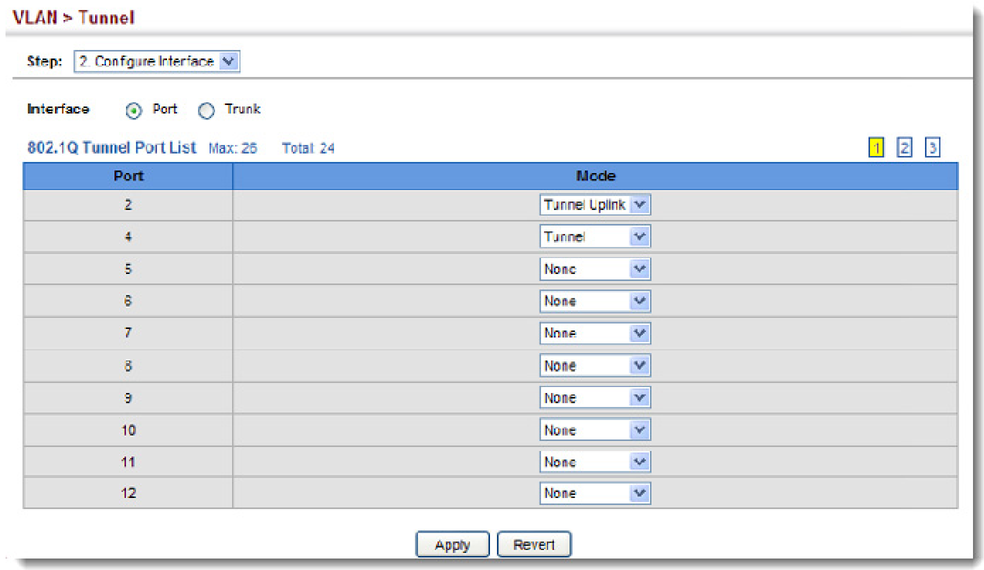
1. Click VLAN, Tunnel.

2. Select Configure Interface from the Step list.

3. Set the mode for any tunnel access port to Tunnel and the tunnel uplink port to Tunnel Uplink.

4. Click Apply.

**Figure 20: Adding an Interface to a QinQ Tunnel**




## PROTOCOL VLANS

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type being used by the inbound packets.

### COMMAND USAGE

■ To configure protocol-based VLANs, follow these steps:

1. First configure VLAN groups for the protocols you want to use (page 890). Although not mandatory, we suggest configuring a separate VLAN for each major protocol running on your network. Do not add port members at this time.

2. Create a protocol group for each of the protocols you want to assign to a VLAN using the Configure Protocol (Add) page.

3. Then map the protocol for each interface to the appropriate VLAN using the Configure Interface (Add) page.

■ When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

## Configuring Protocol VLAN Groups

Use the VLAN > Protocol (Configure Protocol - Add) page to create protocol groups.

### CLI References

- "protocol-vlan protocol-group (Configuring Groups)" on page 912

### Parameters

These parameters are displayed in the web interface:

- **Frame Type** – Choose either Ethernet, RFC 1042, or LLC Other as the frame type used by this protocol.

- **Protocol Type** – Specifies the protocol type to match. The available options are IP, ARP, RARP and IPv6. If LLC Other is chosen for the Frame Type, the only available Protocol Type is IPX Raw.

- **Protocol Group ID** – Protocol Group ID assigned to the Protocol VLAN Group. (Range: 1-2147483647)

---

Traffic which matches IP Protocol Ethernet Frames is mapped to the VLAN (VLAN 1) that has been configured with the switch's administrative IP. IP Protocol Ethernet traffic must not be mapped to another VLAN or you will lose administrative network connectivity to the switch. If lost in this manner, network access can be regained by removing the offending Protocol VLAN rule via the console. Alternately, the switch can be power-cycled, however all unsaved configuration changes will be lost.

---

### Web Interface

To configure a protocol group:

1. Click VLAN, Protocol.

2. Select Configure Protocol from the Step list.

3. Select Add from the Action list.

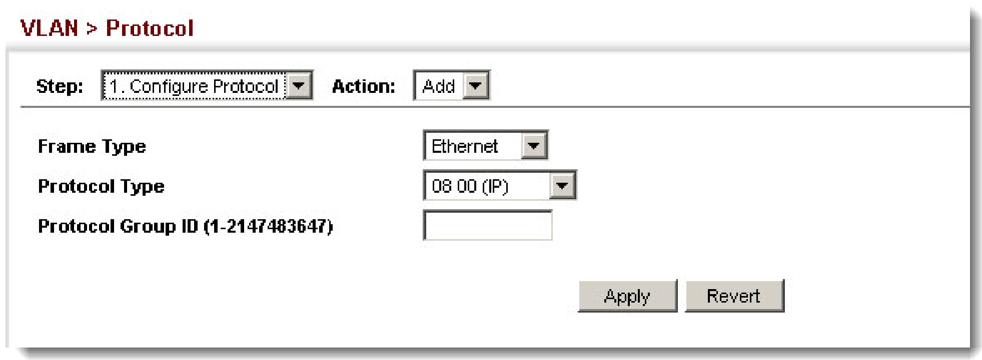
4. Select an entry from the Frame Type list.

5. Select an entry from the Protocol Type list.

6. Enter an identifier for the protocol group.

7. Click Apply.

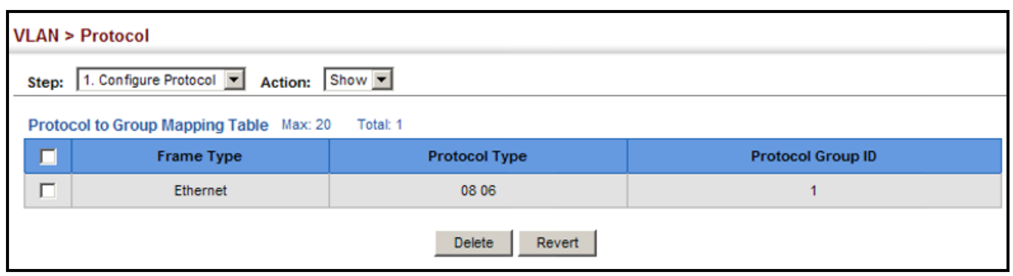
**Figure 21: Configuring Protocol VLANs**




To configure a protocol group:

1. Click VLAN, Protocol.
2. Select Configure Protocol from the Step list.
3. Select Show from the Action list.

**Figure 22: Displaying Protocol VLANs**




## Mapping Protocol Groups to Interfaces

Use the VLAN > Protocol (Configure Interface - Add) page to map a protocol group to a VLAN for each interface that will participate in the group.

### CLI REFERENCES

■ "protocol-vlan protocol-group (Configuring Interfaces)" on page 913

### COMMAND USAGE

■ When creating a protocol-based VLAN, only assign interfaces using this configuration screen. If you assign interfaces using any of the other VLAN menus such as the VLAN Static table (page 142), these interfaces will admit traffic of any protocol type into the associated VLAN.

■ When a frame enters a port that has been assigned to a protocol VLAN, it is processed in the following manner:

- ◆ If the frame is tagged, it will be processed according to the standard rules applied to tagged frames.

- ◆ If the frame is untagged and the protocol type matches, the frame is forwarded to the appropriate VLAN.
- ◆ If the frame is untagged but the protocol type does not match, the frame is forwarded to the default VLAN for this interface.

### PARAMETERS

These parameters are displayed in the web interface:

■**Interface** – Displays a list of ports or trunks.

■**Port** – Port Identifier. (Range: 1-12/14/16/18) depending on the model

■**Trunk** – Trunk Identifier. (Range: 1-32)

■**Protocol Group ID** – Protocol Group ID assigned to the Protocol VLAN Group. (Range: 1-2147483647)

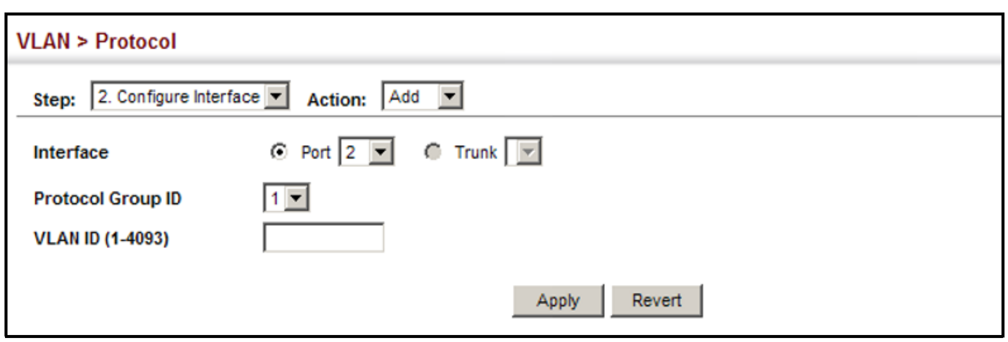
■**VLAN ID** – VLAN to which matching protocol traffic is forwarded. (Range: 1-4093)

### WEB INTERFACE

To map a protocol group to a VLAN for a port or trunk:

1. Click VLAN, Protocol.
2. Select Configure Interface from the Step list.
3. Select Add from the Action list.
4. Select a port or trunk.
5. Enter the identifier for a protocol group.
6. Enter the corresponding VLAN to which the protocol traffic will be forwarded.
7. Click Apply.

**Figure 23: Assigning Interfaces to Protocol VLANs**




To show the protocol groups mapped to a port or trunk:

1. Click VLAN, Protocol.

2. Select Configure Interface from the Step list.

3. Select Show from the Action list.

**Figure 24: Showing the Interface to Protocol Group Mapping**


## CONFIGURING IP SUBNET VLANS

Use the VLAN > IP Subnet page to configure IP subnet-based VLANs.

When using port-based classification, all untagged frames received by a port are classified as belonging to the VLAN whose VID (PVID) is associated with that port.

When IP subnet-based VLAN classification is enabled, the source address of untagged ingress frames are checked against the IP subnet-to-VLAN mapping table. If an entry is found for that subnet, these frames are assigned to the VLAN indicated in the entry. If no IP subnet is matched, the untagged frames are classified as belonging to the receiving port's VLAN ID (PVID).

### CLI REFERENCES

■"Configuring IP Subnet VLANs" on page 915

### COMMAND USAGE

■Each IP subnet can be mapped to only one VLAN ID. An IP subnet consists of an IP address and a mask.

■When an untagged frame is received by a port, the source IP address is checked against the IP subnet-to-VLAN mapping table, and if an entry is found, the corresponding VLAN ID is assigned to the frame. If no mapping is found, the PVID of the receiving port is assigned to the frame.

■The IP subnet cannot be a broadcast or multicast IP address.

■When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

### PARAMETERS

These parameters are displayed in the web interface:

■**IP Address** – The IP address for a subnet. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.

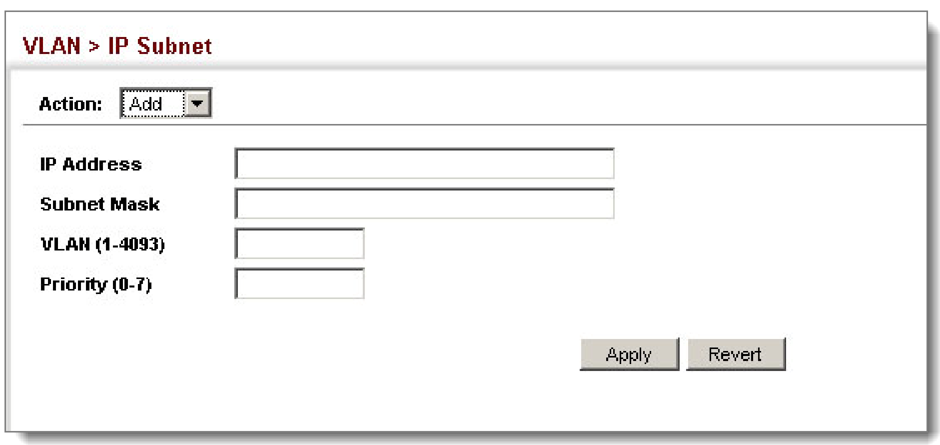
- **Subnet Mask** – This mask identifies the host address bits of the IP subnet.
- **VLAN** – VLAN to which matching IP subnet traffic is forwarded.
  (Range: 1-4093)
- **Priority** – The priority assigned to untagged ingress traffic.
  (Range: 0-7, where 7 is the highest priority; Default: 0)

### WEB INTERFACE

To map an IP subnet to a VLAN:

1. Click VLAN, IP Subnet.
2. Select Add from the Action list.
3. Enter an address in the IP Address field.
4. Enter a mask in the Subnet Mask field.
5. Enter the identifier in the VLAN field. Note that the specified VLAN need not already be configured.
6. Enter a value to assign to untagged frames in the Priority field.
7. Click Apply.

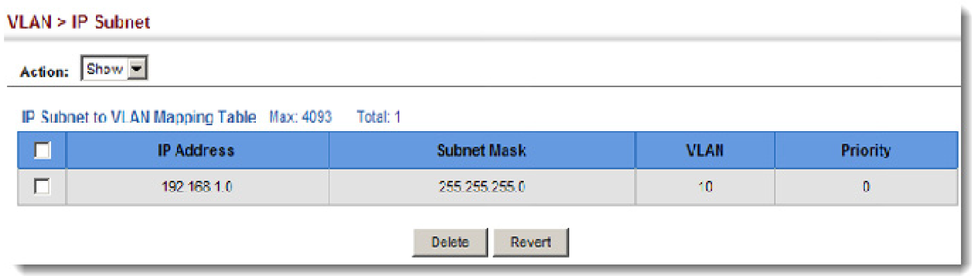
**Figure 25: Configuring IP Subnet VLANs**




To show the configured IP subnet VLANs:

1. Click VLAN, IP Subnet.
2. Select Show from the Action list.

**Figure 26: Showing IP Subnet VLANs**




## CONFIGURING MAC-BASED VLANS

Use the VLAN > MAC-Based page to configure VLAN based on MAC addresses. The MAC-based VLAN feature assigns VLAN IDs to ingress untagged frames according to source MAC addresses.

When MAC-based VLAN classification is enabled, untagged frames received by a port are assigned to the VLAN which is mapped to the frame's source MAC address. When no MAC address is matched, untagged frames are assigned to the receiving port's native VLAN ID (PVID).

### CLI REFERENCES

- "Configuring MAC Based VLANs" on page 917

### COMMAND USAGE

- The MAC-to-VLAN mapping applies to all ports on the switch.
- Source MAC addresses can be mapped to only one VLAN ID.
- Configured MAC addresses cannot be broadcast or multicast addresses.
- When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

### PARAMETERS

These parameters are displayed in the web interface:

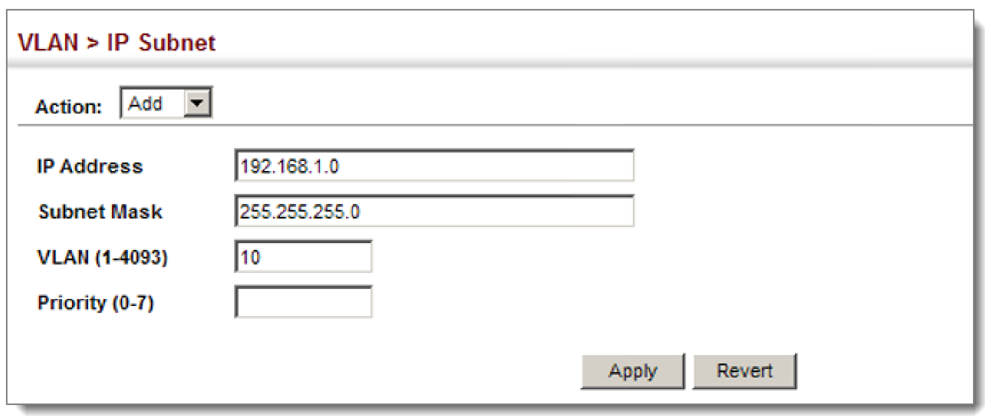
- **MAC Address** – A source MAC address which is to be mapped to a specific VLAN. The MAC address must be specified in the format xx-xx-xx-xx-xx-xx.
- **VLAN** – VLAN to which ingress traffic matching the specified source MAC address is forwarded. (Range: 1-4093)
- **Priority** – The priority assigned to untagged ingress traffic. (Range: 0-7, where 7 is the highest priority; Default: 0)

### WEB INTERFACE

To map a MAC address to a VLAN:

1. Click VLAN, MAC-Based.
2. Select Add from the Action list.
3. Enter an address in the MAC Address field.
4. Enter the identifier in the VLAN field. Note that the specified VLAN need not already be configured.
5. Enter a value to assign to untagged frames in the Priority field.
6. Click Apply.

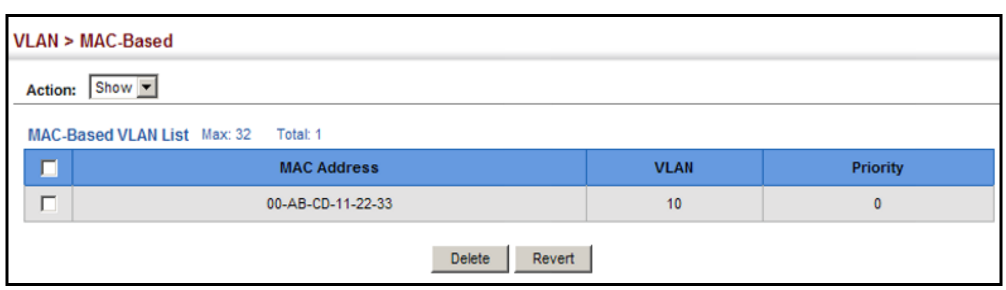
**Figure 27: Configuring MAC-Based VLANs**




To show the MAC addresses mapped to a VLAN:

1. Click VLAN, MAC-Based.
2. Select Show from the Action list.

**Figure 28: Showing MAC-Based VLANs**



# 7 ADDRESS TABLE SETTINGS

Switches store the addresses for all known devices. This information is used to pass traffic directly between the inbound and outbound ports. All the addresses learned by monitoring traffic are stored in the dynamic address table. You can also manually configure static addresses that are bound to a specific port.

This chapter describes the following topics:

- MAC Address Learning – Enables or disables address learning on an interface.
- Static MAC Addresses – Configures static entries in the address table.
- Address Aging Time – Sets timeout for dynamically learned entries.
- Dynamic Address Cache – Shows dynamic entries in the address table.

## CONFIGURING MAC ADDRESS LEARNING

Use the MAC Address > Learning Status page to enable or disable MAC address learning on an interface.

### CLI REFERENCES

- "mac-learning" on page 740

### COMMAND USAGE

- When MAC address learning is disabled, the switch immediately stops learning new MAC addresses on the specified interface. Only incoming traffic with source addresses stored in the static address table (see "Setting Static Addresses" on page 170) will be accepted as authorized to access the network through that interface.
- Dynamic addresses stored in the address table when MAC address learning is disabled are flushed from the system, and no dynamic addresses are subsequently learned until MAC address learning has been re-enabled. Any device not listed in the static address table that attempts to use the interface after MAC learning has been disabled will be prevented from accessing the switch.
- Also note that MAC address learning cannot be disabled if any of the following conditions exist:
  - 802.1X Port Authentication has been globally enabled on the switch (see "Configuring 802.1X Global Settings" on page 307).
  - Security Status (see "Configuring Port Security" on page 304) is enabled on the same interface.

### Parameters

These parameters are displayed in the web interface:

■ **Interface** – Displays a list of ports or trunks.

■ **Port** – Port Identifier. (Range: 1-12/14/16/18) depending on the model

■ **Trunk** – Trunk Identifier. (Range: 1-32)

■ **Status** – The status of MAC address learning. (Default: Enabled)

### Web Interface

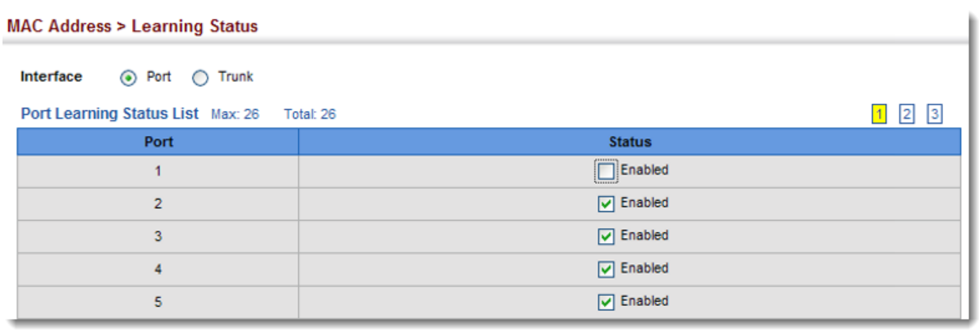
To enable or disable MAC address learning:

1. Click MAC Address, Learning Status.

2. Set the learning status for any interface.

3. Click Apply.

**Figure 1: Configuring MAC Address Learning**




## Setting Static Addresses

Use the MAC Address > Static page to configure static MAC 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.

### CLI References

■ "mac-address-table static" on page 854

### COMMAND USAGE

The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

- Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.
- Static addresses will not be removed from the address table when a given interface link is down.
- A static address cannot be learned on another port until the address is removed from the table.

### PARAMETERS

These parameters are displayed in the web interface:

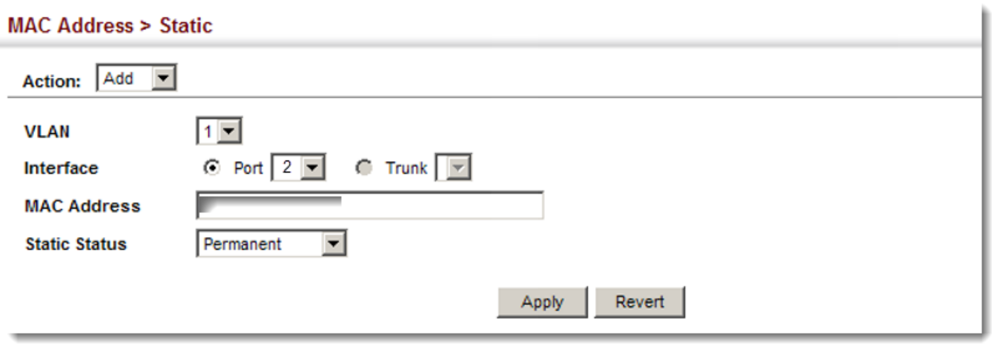
- **VLAN** – ID of configured VLAN. (Range: 1-4093)
- **Interface** – Port or trunk associated with the device assigned a static address.
- **MAC Address** – Physical address of a device mapped to this interface. Enter an address in the form of xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.
- **Static Status** – Sets the time to retain the specified address.
  - Delete-on-reset - Assignment lasts until the switch is reset.
  - Permanent - Assignment is permanent. (This is the default.)

### WEB INTERFACE

To configure a static MAC address:

1. Click MAC Address, Static.
2. Select Add from the Action list.
3. Specify the VLAN, the port or trunk to which the address will be assigned, the MAC address, and the time to retain this entry.
4. Click Apply.

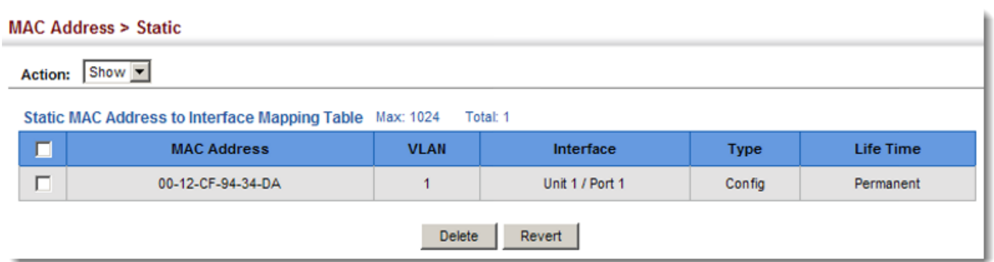
**Figure 2: Configuring Static MAC Addresses**




To show the static addresses in MAC address table:

1. Click MAC Address, Static.
2. Select Show from the Action list.

**Figure 3: Displaying Static MAC Addresses**




## CHANGING THE AGING TIME

Use the MAC Address > Dynamic (Configure Aging) page to set the aging time for entries in the dynamic address table. The aging time is used to age out dynamically learned forwarding information.

### CLI REFERENCES

■"mac-address-table aging-time" on page 853

### PARAMETERS

These parameters are displayed in the web interface:

■**Aging Status** – Enables/disables the function.

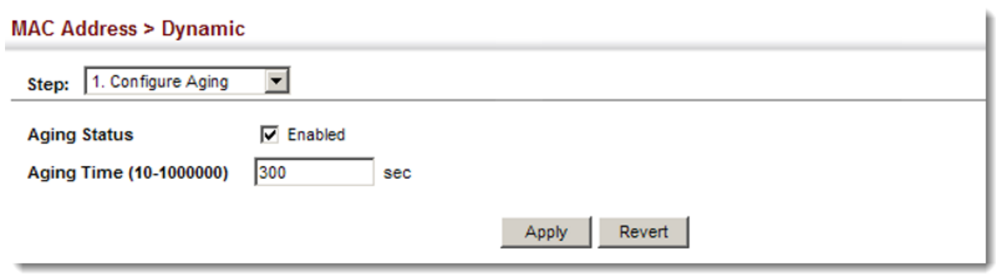
■**Aging Time** – The time after which a learned entry is discarded. (Range: 10-1000000 seconds; Default: 300 seconds)

### WEB INTERFACE

To set the aging time for entries in the dynamic address table:

1. Click MAC Address, Dynamic.
2. Select Configure Aging from the Action list.
3. Modify the aging status if required.
4. Specify a new aging time.
5. Click Apply.

**Figure 4: Setting the Address Aging Time**




## DISPLAYING THE DYNAMIC ADDRESS TABLE

Use the MAC Address > Dynamic (Show Dynamic MAC) page to display the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.

### CLI REFERENCES

- "show mac-address-table" on page 855

### PARAMETERS

These parameters are displayed in the web interface:

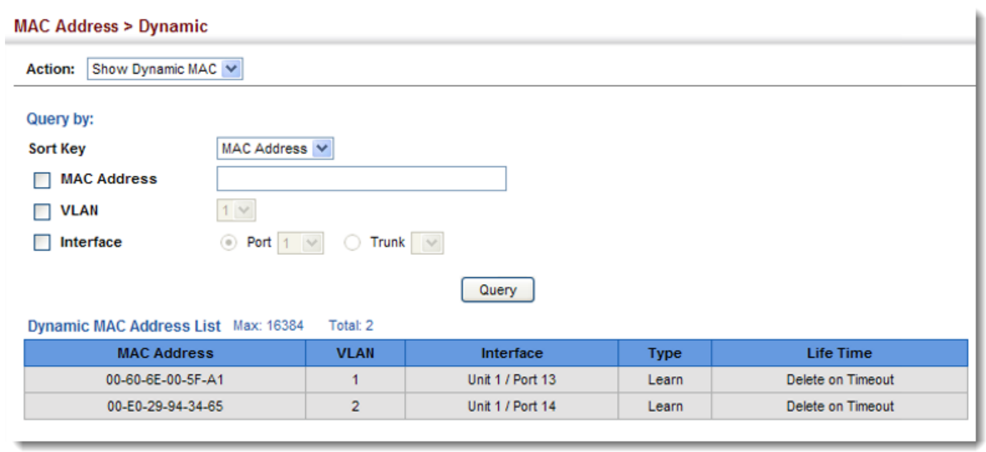
- **Sort Key** - You can sort the information displayed based on MAC address, VLAN or interface (port or trunk).
- **MAC Address** – Physical address associated with this interface.
- **VLAN** – ID of configured VLAN (1-4093).
- **Interface** – Indicates a port or trunk.
- **Type** – Shows that the entries in this table are learned.
- **Life Time** – Shows the time to retain the specified address.

### Web Interface

To show the dynamic address table:

1. Click MAC Address, Dynamic.
2. Select Show Dynamic MAC from the Action list.
3. Select the Sort Key (MAC Address, VLAN, or Interface).
4. Enter the search parameters (MAC Address, VLAN, or Interface).
5. Click Query.

**Figure 5: Displaying the Dynamic MAC Address Table**




## Clearing the Dynamic Address Table

Use the MAC Address > Dynamic (Clear Dynamic MAC) page to remove any learned entries from the forwarding database.

### CLI References

■ "clear mac-address-table dynamic" on page 854

### Parameters

These parameters are displayed in the web interface:

■ **Clear by** – All entries can be cleared; or you can clear the entries for a specific MAC address, all the entries in a VLAN, or all the entries associated with a port or trunk.

### Web Interface

To clear the entries in the dynamic address table:

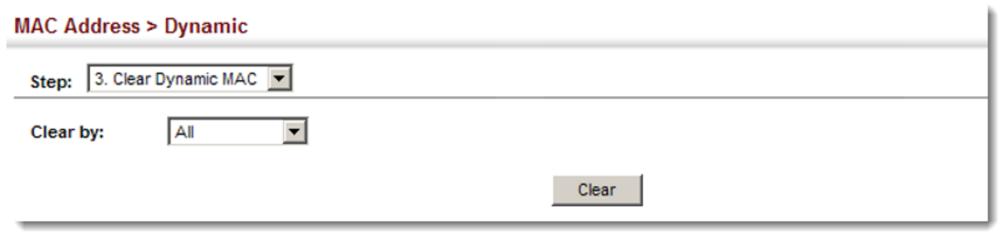
1. Click MAC Address, Dynamic.
2. Select Clear Dynamic MAC from the Action list.

3. Select the method by which to clear the entries (i.e., All, MAC Address, VLAN, or Interface).

4. Enter information in the additional fields required for clearing entries by MAC Address, VLAN, or Interface.

5. Click Clear.

**Figure 6: Clearing Entries in the Dynamic MAC Address Table**



# 8 SPANNING TREE ALGORITHM

This chapter describes the following basic topics:

- Loopback Detection – Configures detection and response to loopback BPDUs.
- Global Settings for STA – Configures global bridge settings for STP, RSTP and MSTP.
- Interface Settings for STA – Configures interface settings for STA, including priority, path cost, link type, and designation as an edge port.
- Global Settings for MSTP – Sets the VLANs and associated priority assigned to an MST instance
- Interface Settings for MSTP – Configures interface settings for MSTP, including priority and path cost.

## OVERVIEW

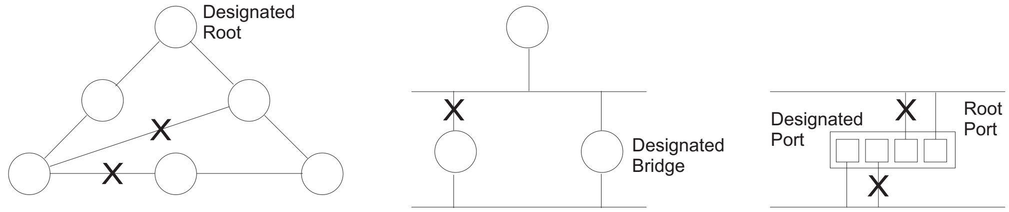
The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

The spanning tree algorithms supported by this switch include these versions:

- STP – Spanning Tree Protocol (IEEE 802.1D)
- RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)
- MSTP – Multiple Spanning Tree Protocol (IEEE 802.1s)

**STP** – STP uses a distributed algorithm to select a bridging device (STP-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

**Figure 1: STP Root Ports and Designated Ports**

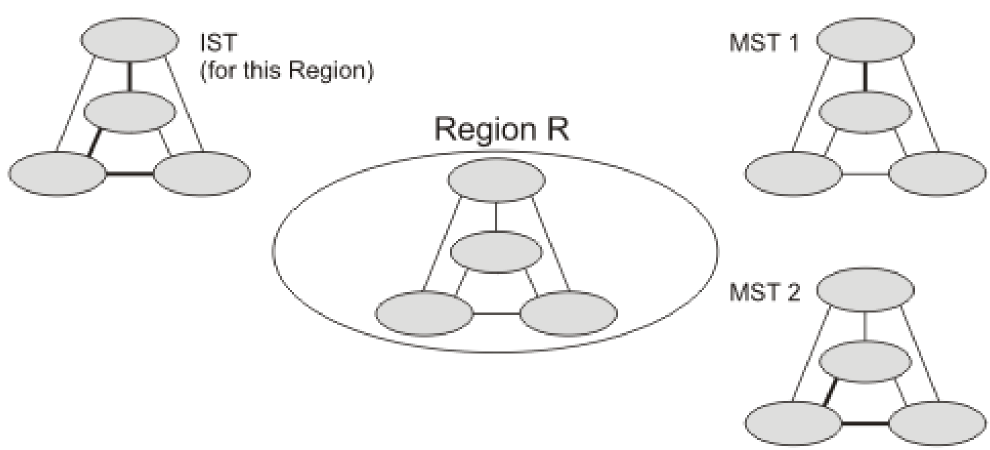



Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

**RSTP** – RSTP is designed as a general replacement for the slower, legacy STP. RSTP is also incorporated into MSTP. RSTP achieves much faster reconfiguration (i.e., around 1 to 3 seconds, compared to 30 seconds or more for STP) by reducing the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails, and retaining the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

**MSTP** – When using STP or RSTP, it may be difficult to maintain a stable path between all VLAN members. Frequent changes in the tree structure can easily isolate some of the group members. MSTP (which is based on RSTP for fast convergence) is designed to support independent spanning trees based on VLAN groups. Using multiple spanning trees can provide multiple forwarding paths and enable load balancing. One or more VLANs can be grouped into a Multiple Spanning Tree Instance (MSTI). MSTP builds a separate Multiple Spanning Tree (MST) for each instance to maintain connectivity among each of the assigned VLAN groups. MSTP then builds a Internal Spanning Tree (IST) for the Region containing all commonly configured MSTP bridges.

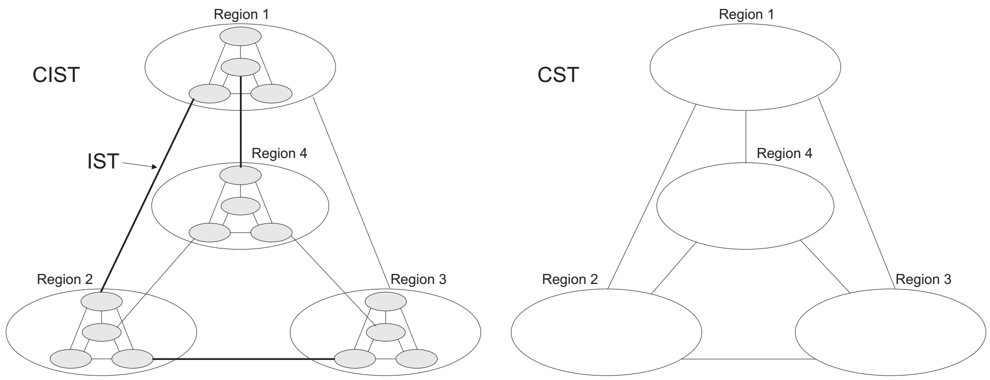
**Figure 2: MSTP Region, Internal Spanning Tree, Multiple Spanning Tree**




An MST Region consists of a group of interconnected bridges that have the same MST Configuration Identifiers (including the Region Name, Revision Level and Configuration Digest – see "Configuring Multiple Spanning Trees" on page 193). An MST Region may contain multiple MSTP Instances. An Internal Spanning Tree (IST) is used to connect all the MSTP switches within an MST region. A Common Spanning

Tree (CST) interconnects all adjacent MST Regions, and acts as a virtual bridge node for communications with STP or RSTP nodes in the global network.

**Figure 3: Common Internal Spanning Tree, Common Spanning Tree, Internal Spanning Tree**




MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree (CIST). The CIST is formed as a result of the running spanning tree algorithm between switches that support the STP, RSTP, MSTP protocols.

Once you specify the VLANs to include in a Multiple Spanning Tree Instance (MSTI), the protocol will automatically build an MSTI tree to maintain connectivity among each of the VLANs. MSTP maintains contact with the global network because each instance is treated as an RSTP node in the Common Spanning Tree (CST).

## CONFIGURING LOOPBACK DETECTION

Use the Spanning Tree > Loopback Detection page to configure loopback detection on an interface. When loopback detection is enabled and a port or trunk receives it's own BPDU, the detection agent drops the loopback BPDU, sends an SNMP trap, and places the interface in discarding mode. This loopback state can be released manually or automatically. If the interface is configured for automatic loopback release, then the port will only be returned to the forwarding state if one of the following conditions is satisfied:

- The interface receives any other BPDU except for it's own, or;
- The interfaces's link status changes to link down and then link up again, or;
- The interface ceases to receive it's own BPDUs in a forward delay interval.

**NOTE:** If loopback detection is not enabled and an interface receives it's own BPDU, then the interface will drop the loopback BPDU according to IEEE Standard 802.1w-2001 9.3.4 (Note 1).

**NOTE:** Loopback detection will not be active if Spanning Tree is disabled on the switch.

**NOTE:** When configured for manual release mode, then a link down/up event will not release the port from the discarding state.

### CLI References

■ "Editing VLAN Groups" on page 890

### Parameters

These parameters are displayed in the web interface:

■ **Interface** – Displays a list of ports or trunks.

■ **Status** – Enables loopback detection on this interface. (Default: Enabled)

■ **Trap** – Enables SNMP trap notification for loopback events on this interface. (Default: Disabled)

■ **Release Mode** – Configures the interface for automatic or manual loopback release. (Default: Auto)

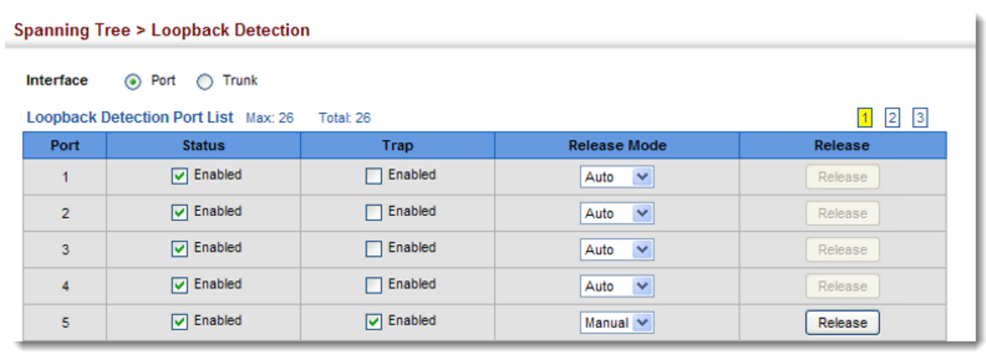
■ **Release** – Allows an interface to be manually released from discard mode. This is only available if the interface is configured for manual release mode.

### Web Interface

To configure loopback detection:

1. Click Spanning Tree, Loopback Detection.
2. Click Port or Trunk to display the required interface type.
3. Modify the required loopback detection attributes.
4. Click Apply

**Figure 4: Configuring Port Loopback Detection**



## CONFIGURING GLOBAL SETTINGS FOR STA

Use the Spanning Tree > STA (Configure Global - Configure) page to configure global settings for the spanning tree that apply to the entire switch.

### CLI REFERENCES

- "Spanning Tree Commands" on page 859

### COMMAND USAGE

- Spanning Tree Protocol[1]

  Uses RSTP for the internal state machine, but sends only 802.1D BPDUs. This creates one spanning tree instance for the entire network. If multiple VLANs are implemented on a network, the path between specific VLAN members may be inadvertently disabled to prevent network loops, thus isolating group members. When operating multiple VLANs, we recommend selecting the MSTP option.

- Rapid Spanning Tree Protocol[1]

  RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:

  - STP Mode – If the switch receives an 802.1D BPDU (i.e., STP BPDU) after a port’s migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.

  - RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

- Multiple Spanning Tree Protocol

  MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.

  - To allow multiple spanning trees to operate over the network, you must configure a related set of bridges with the same MSTP configuration, allowing them to participate in a specific set of spanning tree instances.

  - A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments.

  - Be careful when switching between spanning tree modes. Changing modes stops all spanning-tree instances for the previous mode and restarts the system in the new mode, temporarily disrupting user traffic.

---

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

### PARAMETERS

These parameters are displayed in the web interface:

*Basic Configuration of Global Settings*

■**Spanning Tree Status** – Enables/disables STA on this switch. (Default: Enabled)

■**Spanning Tree Type** – Specifies the type of spanning tree used on this switch:

- ◆ **STP**: Spanning Tree Protocol (IEEE 802.1D); i.e., when this option is selected, the switch will use RSTP set to STP forced compatibility mode).
- ◆ **RSTP**: Rapid Spanning Tree (IEEE 802.1w); RSTP is the default.
- ◆ **MSTP**: Multiple Spanning Tree (IEEE 802.1s)

■**Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. (Note that lower numeric values indicate higher priority.)

- ◆ Default: 32768
- ◆ Range: 0-61440, in steps of 4096
- ◆ Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440

■**BPDU Flooding** – Configures the system to flood BPDUs to all other ports on the switch or just to all other ports in the same VLAN when spanning tree is disabled globally on the switch or disabled on a specific port.

- ◆ To VLAN: Floods BPDUs to all other ports within the receiving port's native VLAN (i.e., as determined by port's PVID). This is the default.
- ◆ To All: Floods BPDUs to all other ports on the switch.

The setting has no effect if BPDU flooding is disabled on a port (see "Configuring Interface Settings for STA").

*Advanced Configuration Settings*

The following attributes are based on RSTP, but also apply to STP since the switch uses a backwards-compatible subset of RSTP to implement STP, and also apply to MSTP which is based on RSTP according to the standard:

■**Path Cost Method** – The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.

- ◆ Long: Specifies 32-bit based values that range from 1-200,000,000. (This is the default.)
- ◆ Short: Specifies 16-bit based values that range from 1-65535.

■ **Transmission Limit** – The maximum transmission rate for BPDUs is specified by setting the minimum interval between the transmission of consecutive protocol messages. (Range: 1-10; Default: 3)

*When the Switch Becomes Root*

■ **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.

- Default: 2
- Minimum: 1
- Maximum: The lower of 10 or [(Max. Message Age / 2) -1]

■ **Maximum Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to "ports" in this section mean "interfaces," which includes both ports and trunks.)

- Default: 20
- Minimum: The higher of 6 or [2 x (Hello Time + 1)]
- Maximum: The lower of 40 or [2 x (Forward Delay - 1)]

■ **Forward Delay** – The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.

- Default: 15
- Minimum: The higher of 4 or [(Max. Message Age / 2) + 1]
- Maximum: 30

*Configuration Settings for MSTP*

■ **Max Instance Numbers** – The maximum number of MSTP instances to which this switch can be assigned.

■ **Configuration Digest** – An MD5 signature key that contains the VLAN ID to MST ID mapping table. In other words, this key is a mapping of all VLANs to the CIST.

■ **Region Revision**[2] – The revision for this MSTI. (Range: 0-65535; Default: 0)

■ **Region Name**[2] – The name for this MSTI. (Maximum length: 32 characters; switch's MAC address)

■ **Max Hop Count** – The maximum number of hops allowed in the MST region before a BPDU is discarded. (Range: 1-40; Default: 20)

2. The MST name and revision number are both required to uniquely identify an MST region.

### WEB INTERFACE

To configure global STA settings:

1. Click Spanning Tree, STA.
2. Select Configure Global from the Step list.
3. Select Configure from the Action list.
4. Modify any of the required attributes. Note that the parameters displayed for the spanning tree types (STP, RSTP, MSTP) varies as described in the preceding section.
5. Click Apply

**Figure 5: Configuring Global Settings for STA** (STP)

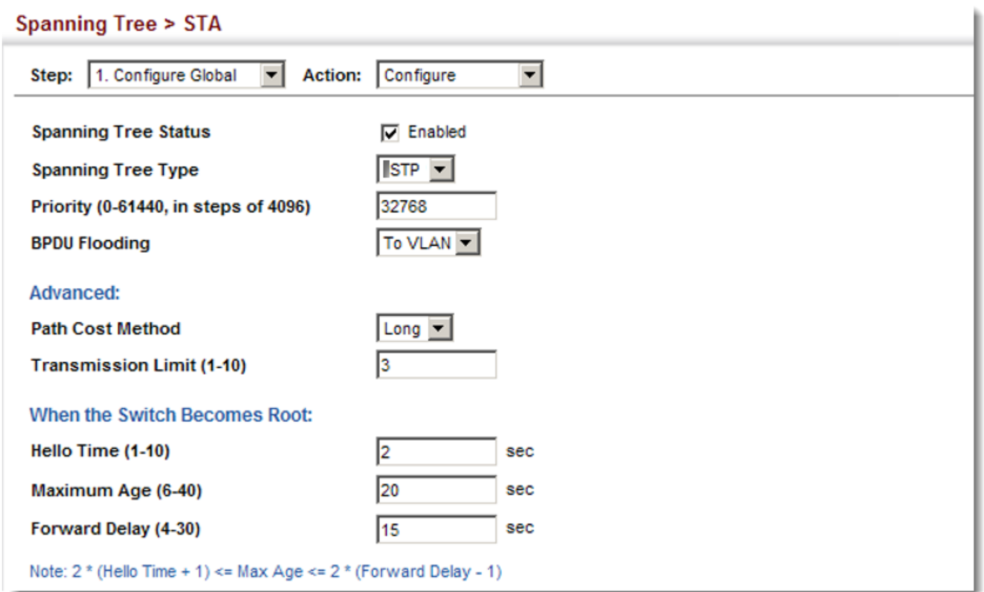


**Figure 6: Configuring Global Settings for STA** (RSTP)

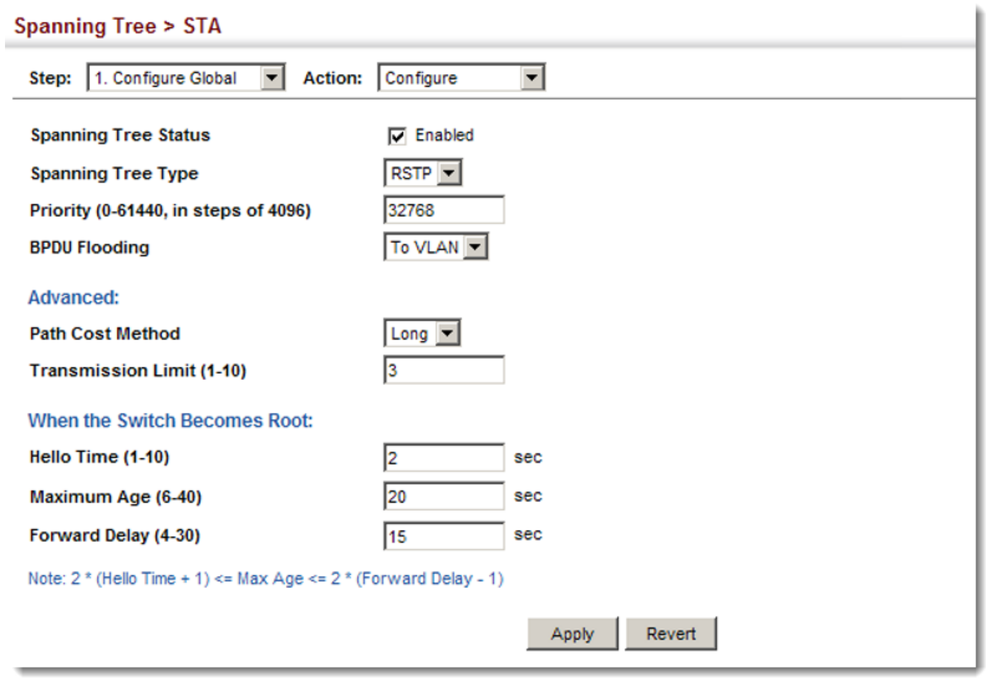
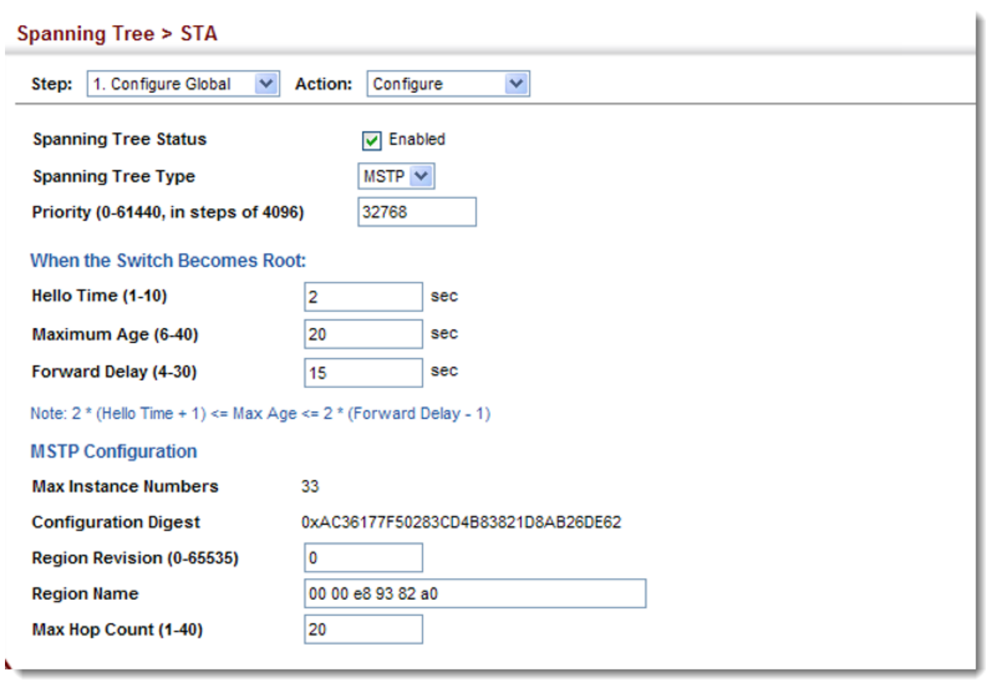



**Figure 7: Configuring Global Settings for STA** (MSTP)



## DISPLAYING GLOBAL SETTINGS FOR STA

Use the Spanning Tree > STA (Configure Global - Show Information) page to display a summary of the current bridge STA information that applies to the entire switch.

### CLI REFERENCES

■"show spanning-tree" on page 881
■"show spanning-tree mst configuration" on page 883

### PARAMETERS

The parameters displayed in the web interface are described in the preceding section, except for the following items:

■**Bridge ID** – A unique identifier for this bridge, consisting of the bridge priority, the MST Instance ID 0 for the Common Spanning Tree when spanning tree type is set to MSTP, and MAC address (where the address is taken from the switch system).

■**Designated Root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.

■**Root Port** – The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.

■**Root Path Cost** – The path cost from the root port on this switch to the root device.

■**Configuration Changes** – The number of times the Spanning Tree has been reconfigured.

■**Last Topology Change** – Time since the Spanning Tree was last reconfigured.

### WEB INTERFACE

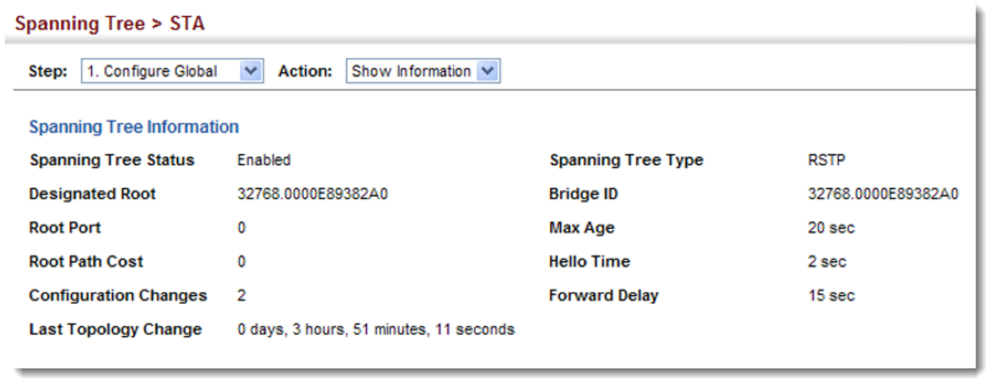
To display global STA settings:

1. Click Spanning Tree, STA.

2. Select Configure Global from the Step list.

3. Select Show Information from the Action list.

**Figure 8: Displaying Global Settings for STA**




## CONFIGURING INTERFACE SETTINGS FOR STA

Use the Spanning Tree > STA (Configure Interface - Configure) page to configure RSTP and MSTP attributes for specific interfaces, including port priority, path cost, link type, and edge port. You may use a different priority or path cost for ports of the same media type to indicate the preferred path, link type to indicate a point-to-point connection or shared-media connection, and edge port to indicate if the attached device can support fast forwarding. (References to “ports” in this section means “interfaces,” which includes both ports and trunks.)

### CLI REFERENCES

- "Spanning Tree Commands" on page 859

### PARAMETERS

These parameters are displayed in the web interface:

- **Interface** – Displays a list of ports or trunks.
- **Spanning Tree** – Enables/disables STA on this interface. (Default: Enabled)
- **BPDU Flooding** - Enables/disables the flooding of BPDUs to other ports when global spanning tree is disabled (page 181) or when spanning tree is disabled on specific port. When flooding is enabled, BPDUs are flooded to all other ports on the switch or to all other ports within the receiving port’s native VLAN as specified by the Spanning Tree BPDU Flooding attribute (page 181).
- **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.
  - Default: 128
  - Range: 0-240, in steps of 16

- **Admin Path Cost** – This parameter is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Also, not that path cost takes precedence over port priority. (Range: 0 for auto-configuration, 1-65535 for the short path cost method[3], 1-200,000,000 for the long path cost method)

  By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

**Table 1: Recommended STA Path Cost Range**

| Port Type | IEEE 802.1D-1998 | IEEE 802.1w-2001 |
|---|---|---|
| Gigabit Ethernet | 3-10 | 2,000-200,000 |
| 10G Ethernet | 200-20,000 | 200-20,000 |

**Table 2: Default STA Path Costs**

| Port Type | Short Path Cost (IEEE 802.1D-1998) | Long Path Cost (802.1D-2004) |
|---|---|---|
| Gigabit Ethernet | 10,000 | 10,000 |
| 10G Ethernet | 1,000 | 1,000 |

- **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.)
- **Root Guard** – STA allows a bridge with a lower bridge identifier (or same identifier and lower MAC address) to take over as the root bridge at any time. Root Guard can be used to ensure that the root bridge is not formed at a suboptimal location. Root Guard should be enabled on any designated port connected to low-speed bridges which could potentially overload a slower link by taking over as the root port and forming a new spanning tree topology. It could also be used to form a border around part of the network where the root bridge is allowed. (Default: Disabled)
- **Admin Edge Port** – Since end nodes **cannot** cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and

3. Refer to "Configuring Global Settings for STA" on page 181 for information on setting the path cost method.

also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device. (Default: Disabled)

- **Enabled** – Manually configures a port as an Edge Port.
- **Disabled** – Disables the Edge Port setting.
- **Auto** – The port will be automatically configured as an edge port if the edge delay time expires without receiving any RSTP or MSTP BPDUs. Note that edge delay time (802.1D-2004 17.20.4) equals the protocol migration time if a port's link type is point-to-point (which is 3 seconds as defined in IEEE 802.3D-2004 17.20.4); otherwise it equals the spanning tree's maximum age for configuration messages (see maximum age under "Configuring Global Settings for STA" on page 181).

An interface cannot function as an edge port under the following conditions:

- If spanning tree mode is set to STP (page 181), edge-port mode cannot automatically transition to operational edge-port state using the automatic setting.
- If loopback detection is enabled (page 179) and a loopback BPDU is detected, the interface cannot function as an edge port until the loopback state is released.
- If an interface is in forwarding state and its role changes, the interface cannot continue to function as an edge port even if the edge delay time has expired.
- If the port does not receive any BPDUs after the edge delay timer expires, its role changes to designated port and it immediately enters forwarding state (see "Displaying Interface Settings for STA" on page 190).

- **BPDU Guard**[4] – This feature protects edge ports from receiving BPDUs. It prevents loops by shutting down an edge port when a BPDU is received instead of putting it into the spanning tree discarding state. In a valid configuration, configured edge ports should not receive BPDUs. If an edge port receives a BPDU an invalid configuration exists, such as a connection to an unauthorized device. The BPDU guard feature provides a secure response to invalid configurations because an administrator must manually enable the port. (Default: Disabled)
- **BPDU Filter**[4] – BPDU filtering allows you to avoid transmitting BPDUs on configured edge ports that are connected to end nodes. By default, STA sends BPDUs to all ports regardless of whether administrative edge is enabled on a port. BDPU filtering is configured on a per-port basis. (Default: Disabled)
- **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)

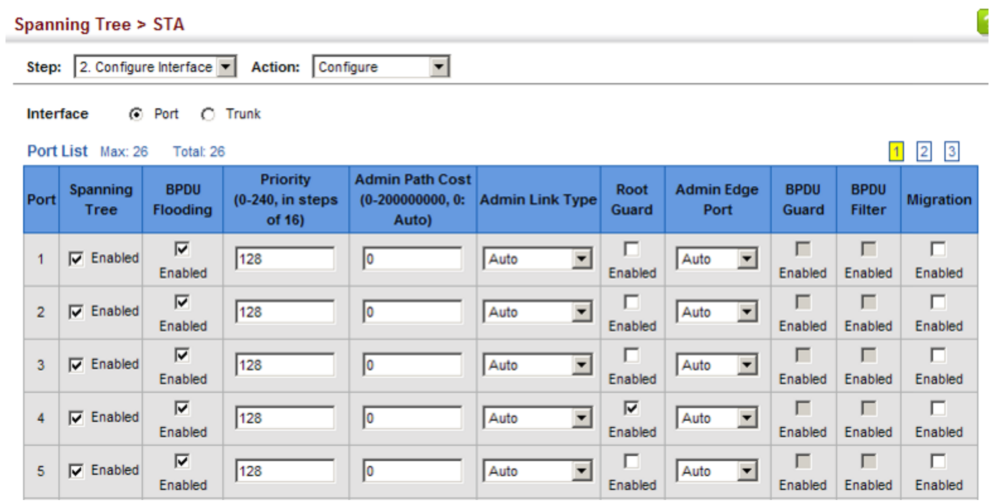
4. Admin Edge Port must be enabled to use this feature.

### WEB INTERFACE

To configure interface settings for STA:

1. Click Spanning Tree, STA.
2. Select Configure Interface from the Step list.
3. Select Configure from the Action list.
4. Modify any of the required attributes.
5. Click Apply.

**Figure 9: Configuring Interface Settings for STA**




## DISPLAYING INTERFACE SETTINGS FOR STA

Use the Spanning Tree > STA (Configure Interface - Show Information) page to display the current status of ports or trunks in the Spanning Tree.

### CLI REFERENCES

■"show spanning-tree" on page 881

### PARAMETERS

These parameters are displayed in the web interface:

■**Spanning Tree** – Shows if STA has been enabled on this interface.

■**BPDU Flooding** – Shows if BPDUs will be flooded to other ports when spanning tree is disabled globally on the switch or disabled on a specific port.

■**STA Status** – Displays current state of this port within the Spanning Tree:

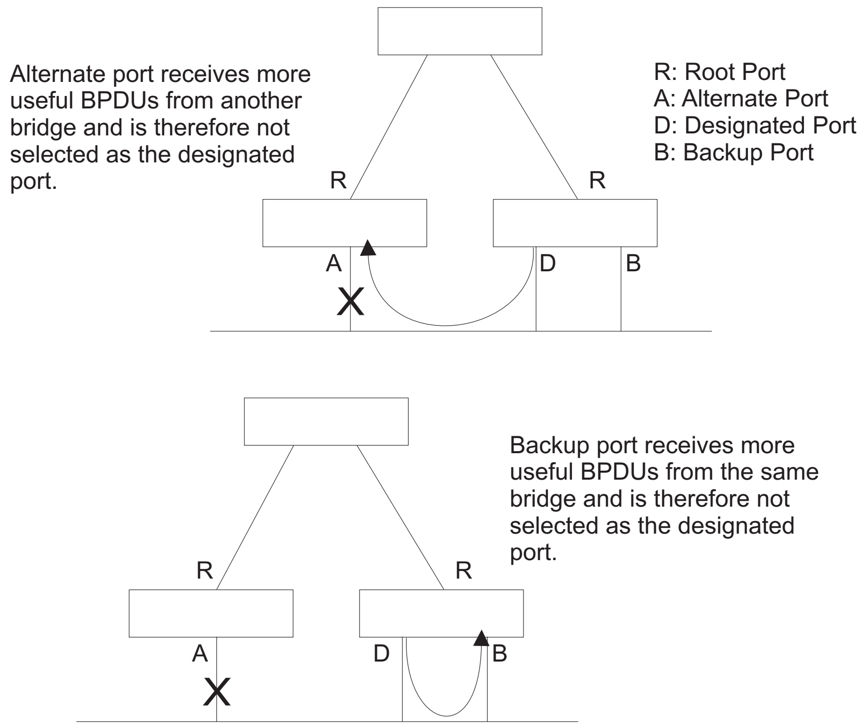
- **Discarding** - Port receives STA configuration messages, but does not forward packets.
- **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
- **Forwarding** - Port forwards packets, and continues learning addresses.

The rules defining port status are:

- A port on a network segment with no other STA compliant bridging device is always forwarding.
- If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is discarding.
- All ports are discarding when the switch is booted, then some of them change state to learning, and then to forwarding.

- **Forward Transitions** – The number of times this port has transitioned from the Learning state to the Forwarding state.
- **Designated Cost** – The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
- **Designated Bridge** – The bridge priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.
- **Designated Port** – The port priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.
- **Oper Path Cost** – The contribution of this port to the path cost of paths towards the spanning tree root which include this port.
- **Oper Link Type** – The operational point-to-point status of the LAN segment attached to this interface. This parameter is determined by manual configuration or by auto-detection, as described for Admin Link Type in STA Port Configuration on page 187.
- **Oper Edge Port** – This parameter is initialized to the setting for Admin Edge Port in STA Port Configuration on page 187 (i.e., true or false), but will be set to false if a BPDU is received, indicating that another bridge is attached to this port.
- **Port Role** – Roles are assigned according to whether the port is part of the active topology connecting the bridge to the root bridge (i.e., **root** port), connecting a LAN through the bridge to the root bridge (i.e., **designated** port), is the MSTI regional root (i.e., **master** port), or is an **alternate** or **backup** port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed. The role is set to disabled (i.e., **disabled** port) if a port has no role within the spanning tree.

**Figure 10: STA Port Roles**

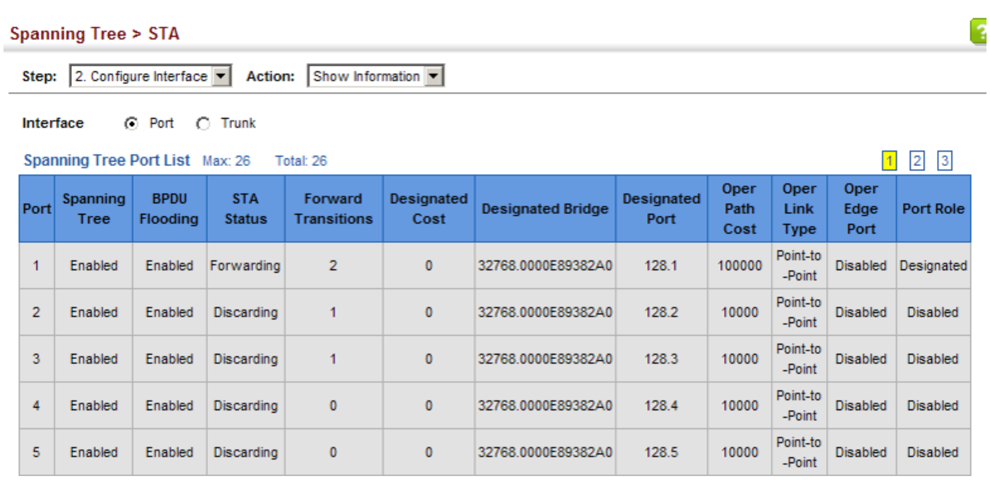



### WEB INTERFACE

To display interface settings for STA:

1. Click Spanning Tree, STA.
2. Select Configure Interface from the Step list.
3. Select Show Information from the Action list.

**Figure 11: Displaying Interface Settings for STA**



Spanning Tree > STA

Step: 2. Configure Interface   Action: Show Information

Interface ◉ Port ○ Trunk

Spanning Tree Port List Max: 26 Total: 26   1 2 3

| Port | Spanning Tree | BPDU Flooding | STA Status | Forward Transitions | Designated Cost | Designated Bridge | Designated Port | Oper Path Cost | Oper Link Type | Oper Edge Port | Port Role |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Enabled | Enabled | Forwarding | 2 | 0 | 32768.0000E89382A0 | 128.1 | 100000 | Point-to -Point | Disabled | Designated |
| 2 | Enabled | Enabled | Discarding | 1 | 0 | 32768.0000E89382A0 | 128.2 | 10000 | Point-to -Point | Disabled | Disabled |
| 3 | Enabled | Enabled | Discarding | 1 | 0 | 32768.0000E89382A0 | 128.3 | 10000 | Point-to -Point | Disabled | Disabled |
| 4 | Enabled | Enabled | Discarding | 0 | 0 | 32768.0000E89382A0 | 128.4 | 10000 | Point-to -Point | Disabled | Disabled |
| 5 | Enabled | Enabled | Discarding | 0 | 0 | 32768.0000E89382A0 | 128.5 | 10000 | Point-to -Point | Disabled | Disabled |

## CONFIGURING MULTIPLE SPANNING TREES

Use the Spanning Tree > MSTP (Configure Global) page to create an MSTP instance, or to add VLAN groups to an MSTP instance.

### CLI REFERENCES

- "Spanning Tree Commands" on page 859

### COMMAND USAGE

MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.

By default all VLANs are assigned to the Internal Spanning Tree (MST Instance 0) that connects all bridges and LANs within the MST region. This switch supports up to 33 instances. You should try to group VLANs which cover the same general area of your network. However, remember that you must configure all bridges within the same MSTI Region (page 181) with the same set of instances, and the same instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each MSTI region as a single node, connecting all regions to the Common Spanning Tree.

To use multiple spanning trees:

1. Set the spanning tree type to MSTP (page 181).
2. Enter the spanning tree priority for the selected MST instance on the Spanning Tree > MSTP (Configure Global - Add) page.
3. Add the VLANs that will share this MSTI on the Spanning Tree > MSTP (Configure Global - Add Member) page.

**NOTE:** All VLANs are automatically added to the IST (Instance 0).

To ensure that the MSTI maintains connectivity across the network, you must configure a related set of bridges with the same MSTI settings.

### PARAMETERS

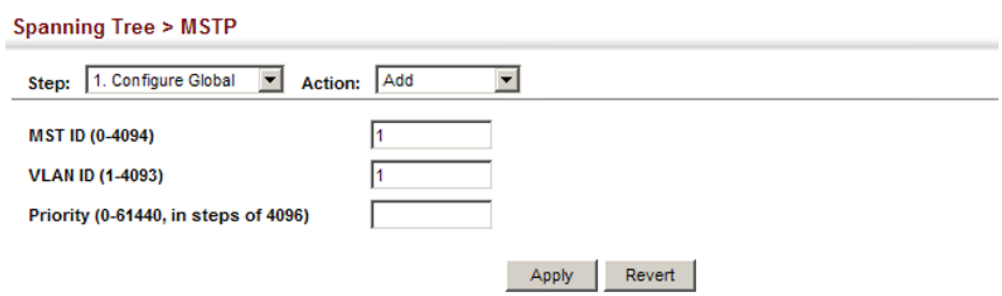
These parameters are displayed in the web interface:

- **MST ID** – Instance identifier to configure. (Range: 0-4094)
- **VLAN ID** – VLAN to assign to this MST instance. (Range: 1-4093)
- **Priority** – The priority of a spanning tree instance. (Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440; Default: 32768)

**WEB INTERFACE**
To create instances for MSTP:

1. Click Spanning Tree, MSTP.
2. Select Configure Global from the Step list.
3. Select Add from the Action list.
4. Specify the MST instance identifier and the initial VLAN member. Additional member can be added using the Spanning Tree > MSTP (Configure Global - Add Member) page. If the priority is not specified, the default value 32768 is used.
5. Click Apply.

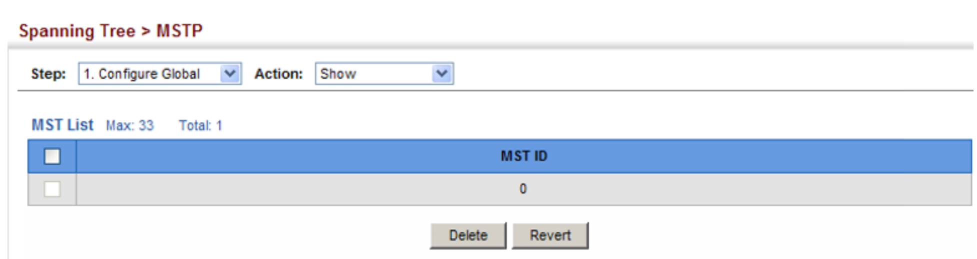
**Figure 12: Creating an MST Instance**




To show the MSTP instances:

1. Click Spanning Tree, MSTP.
2. Select Configure Global from the Step list.
3. Select Show from the Action list.

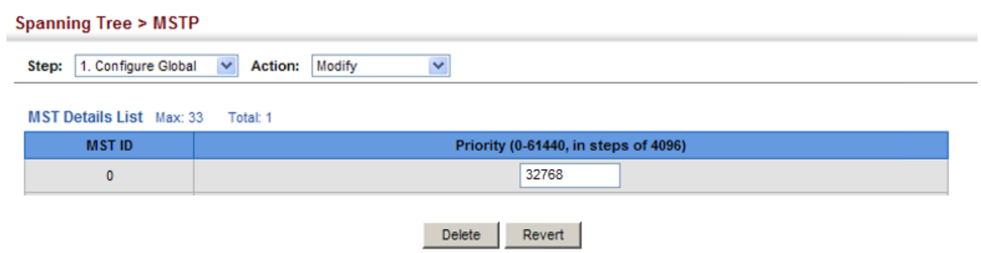
**Figure 13: Displaying MST Instances**



To modify the priority for an MST instance:

1. Click Spanning Tree, MSTP.
2. Select Configure Global from the Step list.
3. Select Modify from the Action list.
4. Modify the priority for an MSTP Instance.
5. Click Apply.

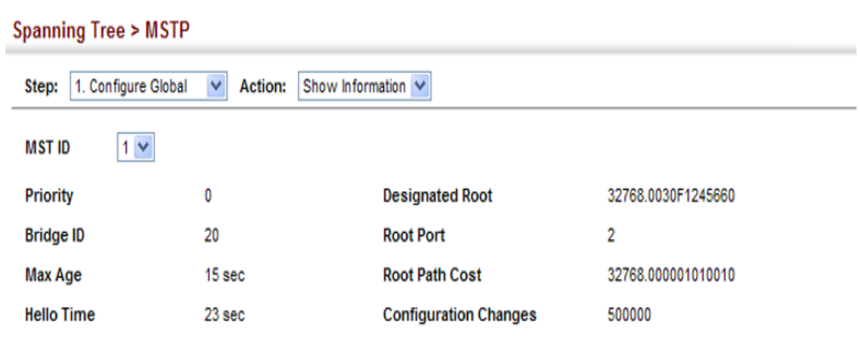
**Figure 14: Modifying the Priority for an MST Instance**




To display global settings for MSTP:

1. Click Spanning Tree, MSTP.
2. Select Configure Global from the Step list.
3. Select Show Information from the Action list.
4. Select an MST ID. The attributes displayed on this page are described under "Displaying Global Settings for STA" on page 186.

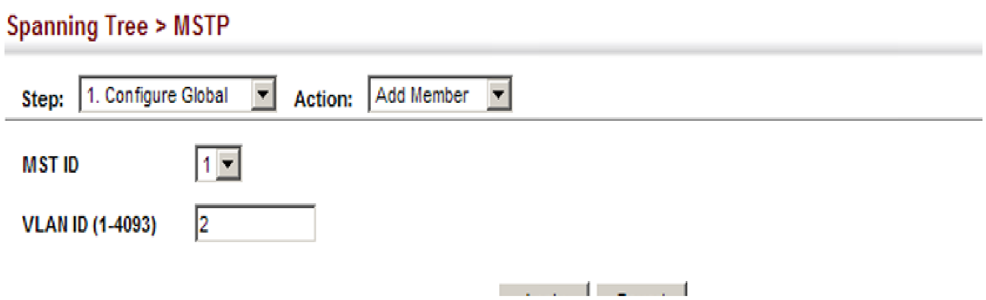
**Figure 15: Displaying Global Settings for an MST Instance**



To add additional VLAN groups to an MSTP instance:

1. Click Spanning Tree, MSTP.
2. Select Configure Global from the Step list.
3. Select Add Member from the Action list.
4. Select an MST instance from the MST ID list.
5. Enter the VLAN group to add to the instance in the VLAN ID field. Note that the specified member does not have to be a configured VLAN.
6. Click Apply

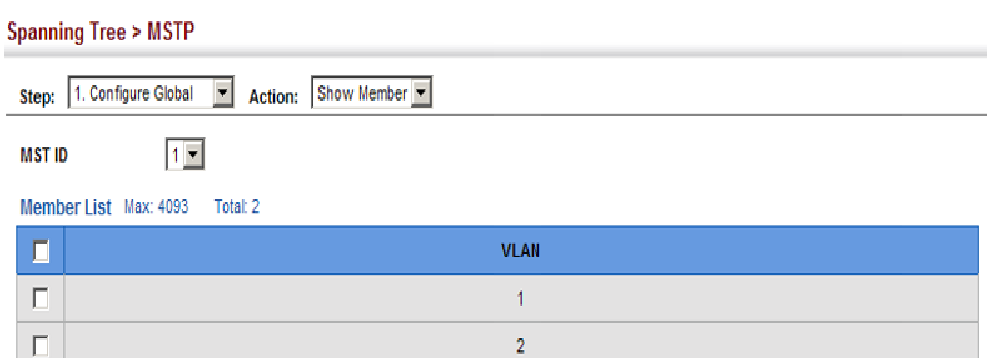
**Figure 16: Adding a VLAN to an MST Instance**




To show the VLAN members of an MSTP instance:

1. Click Spanning Tree, MSTP.
2. Select Configure Global from the Step list.
3. Select Show Member from the Action list.

**Figure 17: Displaying Members of an MST Instance**



## CONFIGURING INTERFACE SETTINGS FOR MSTP

Use the Spanning Tree > MSTP (Configure Interface - Configure) page to configure the STA interface settings for an MST instance.

### CLI REFERENCES

- "Spanning Tree Commands" on page 859

### PARAMETERS

These parameters are displayed in the web interface:

- **MST Instance ID** – Instance identifier to configure. (Default: 0)
- **Interface** – Displays a list of ports or trunks.
- **STA Status** – Displays the current state of this interface within the Spanning Tree. (See "Displaying Interface Settings for STA" on page 190 for additional information.)
  - **Discarding** – Port receives STA configuration messages, but does not forward packets.
  - **Learning** – Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** – Port forwards packets, and continues learning addresses.
- **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. (Default: 128; Range: 0-240, in steps of 16)
- **Admin MST Path Cost** – This parameter is used by the MSTP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to short (page 3-63), the maximum path cost is 65,535.

  By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost “0” is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

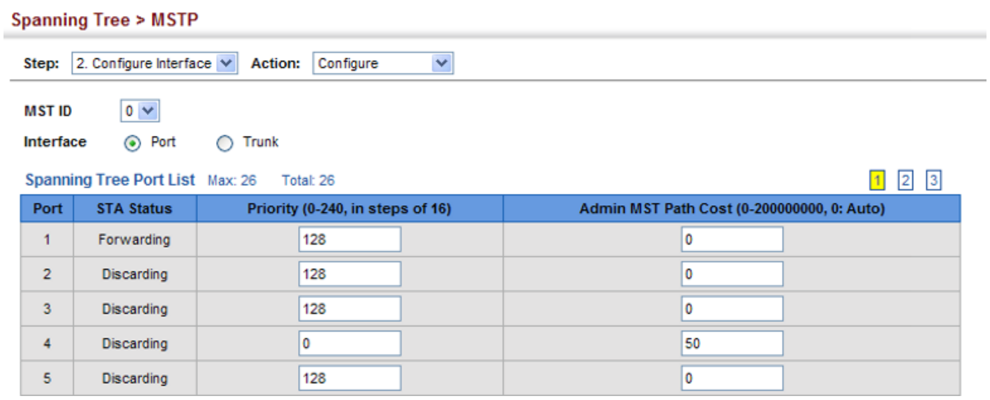
  The recommended range is listed in Table 1 on page 188.
  The default path costs are listed in Table 2 on page 188.

### WEB INTERFACE

To configure MSTP parameters for a port or trunk:

1. Click Spanning Tree, MSTP.
2. Select Configure Interface from the Step list.
3. Select Configure from the Action list.
4. Enter the priority and path cost for an interface
5. Click Apply.

**Figure 18: Configuring MSTP Interface Settings**

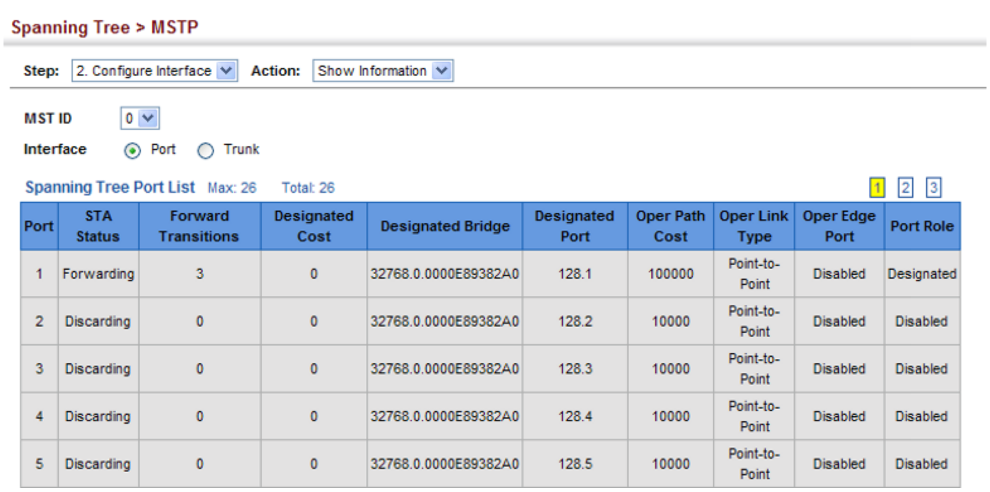



| Port | STA Status | Priority (0-240, in steps of 16) | Admin MST Path Cost (0-200000000, 0: Auto) |
|---|---|---|---|
| 1 | Forwarding | 128 | 0 |
| 2 | Discarding | 128 | 0 |
| 3 | Discarding | 128 | 0 |
| 4 | Discarding | 0 | 50 |
| 5 | Discarding | 128 | 0 |

To display MSTP parameters for a port or trunk:

1. Click Spanning Tree, MSTP.
2. Select Configure Interface from the Step list.
3. Select Show Information from the Action list.

**Figure 19: Displaying MSTP Interface Settings**




| Port | STA Status | Forward Transitions | Designated Cost | Designated Bridge | Designated Port | Oper Path Cost | Oper Link Type | Oper Edge Port | Port Role |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Forwarding | 3 | 0 | 32768.0.0000E89382A0 | 128.1 | 100000 | Point-to-Point | Disabled | Designated |
| 2 | Discarding | 0 | 0 | 32768.0.0000E89382A0 | 128.2 | 10000 | Point-to-Point | Disabled | Disabled |
| 3 | Discarding | 0 | 0 | 32768.0.0000E89382A0 | 128.3 | 10000 | Point-to-Point | Disabled | Disabled |
| 4 | Discarding | 0 | 0 | 32768.0.0000E89382A0 | 128.4 | 10000 | Point-to-Point | Disabled | Disabled |
| 5 | Discarding | 0 | 0 | 32768.0.0000E89382A0 | 128.5 | 10000 | Point-to-Point | Disabled | Disabled |

# 9 RATE LIMIT CONFIGURATION

Use the Traffic > Rate Limit page to apply rate limiting to ingress or egress ports. This function allows the network manager to control the maximum rate for traffic received or transmitted on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or 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.

### CLI REFERENCES

■"Rate Limit Commands" on page 837

### PARAMETERS

These parameters are displayed in the web interface:

■**Port** – Displays the port number.

■**Type** – Indicates the port type. (1000Base-T, 1000Base SFP, or 10G)

■**Status** – Enables or disables the rate limit. (Default: Disabled)

■**Rate** – Sets the rate limit level. (Range: 64 - 1,000,000 kbits per second for Gigabit Ethernet ports; 64 - 10,000,000 kbits per second for 10G ports)

### WEB INTERFACE

To configure rate limits:

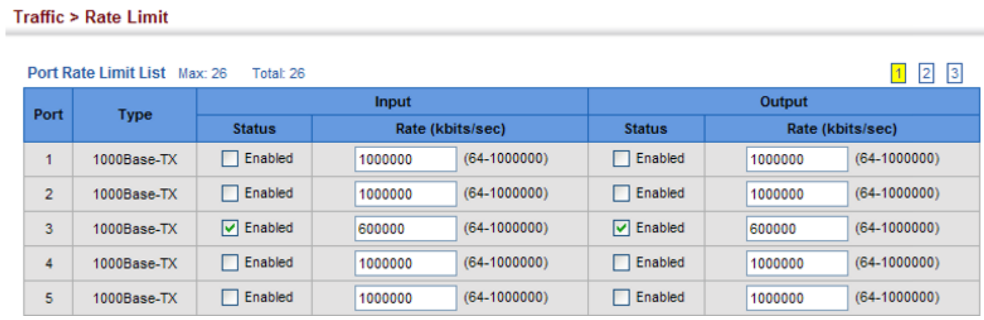
1. Click Traffic, Rate Limit.

2. Enable the Rate Limit Status for the required ports.

3. Set the rate limit for the individual ports.

4. Click Apply.

**Figure 1: Configuring Rate Limits**



Traffic > Rate Limit

Port Rate Limit List Max: 26 Total: 26

1 2 3

| Port | Type | Input | | Output | |
|---|---|---|---|---|---|
| | | Status | Rate (kbits/sec) | Status | Rate (kbits/sec) |
| 1 | 1000Base-TX | ☐ Enabled | 1000000 (64-1000000) | ☐ Enabled | 1000000 (64-1000000) |
| 2 | 1000Base-TX | ☐ Enabled | 1000000 (64-1000000) | ☐ Enabled | 1000000 (64-1000000) |
| 3 | 1000Base-TX | ☑ Enabled | 600000 (64-1000000) | ☑ Enabled | 600000 (64-1000000) |
| 4 | 1000Base-TX | ☐ Enabled | 1000000 (64-1000000) | ☐ Enabled | 1000000 (64-1000000) |
| 5 | 1000Base-TX | ☐ Enabled | 1000000 (64-1000000) | ☐ Enabled | 1000000 (64-1000000) |

# 10 STORM CONTROL CONFIGURATION

Use the Traffic > Storm Control page to configure broadcast, multicast, and unknown unicast storm control thresholds. Traffic 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 traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from traffic storms by setting a threshold for broadcast, multicast or unknown unicast traffic. Any packets exceeding the specified threshold will then be dropped.

### CLI REFERENCES

■"switchport packet-rate" on page 813

### COMMAND USAGE

■Broadcast Storm Control is enabled by default.

■Broadcast control does not effect IP multicast traffic.

■When traffic exceeds the threshold specified for broadcast and multicast or unknown unicast traffic, packets exceeding the threshold are dropped until the rate falls back down beneath the threshold.

■The rate limits set by this function are also used by automatic storm control when the control response is set to rate limiting by the auto-traffic-control action command.

■Using both rate limiting and storm control on the same interface may lead to unexpected results. For example, suppose broadcast storm control is set to 500 pps by the command “switchport broadcast packet-rate 500" and the rate limit is set to 200 Mbps by the command “rate-limit input 20" on a port. Since 200 Mbps is 1/5 of line speed (1000 Mbps), the received rate will actually be 100 pps, or 1/5 of the 500 pps limit set by the storm control command. It is therefore not advisable to use both of these commands on the same interface.

### PARAMETERS

These parameters are displayed in the web interface:

■**Interface** – Displays a list of ports or trunks.

■**Type** – Indicates interface type. (1000Base-T, SFP, or 10G)

■**Unknown Unicast** – Specifies storm control for unknown unicast traffic.

■**Multicast** – Specifies storm control for multicast traffic.

■**Broadcast** – Specifies storm control for broadcast traffic.

- **Status** – Enables or disables storm control. (Default: Enabled for broadcast storm control, disabled for multicast and unknown unicast storm control)

- **Rate** – Threshold level as a rate; i.e., packets per second. (Range: 500-262143 packets per second; Default: 500 pps for broadcast traffic, 262143 pps for unknown unicast and multicast traffic)

### WEB INTERFACE

To configure broadcast storm control:

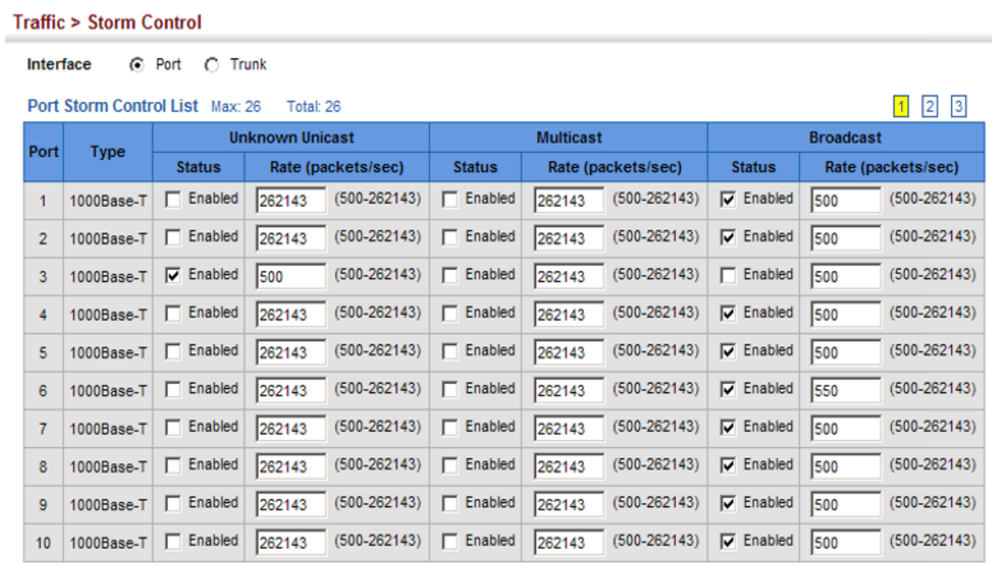
Click Traffic, Storm Control.

Set the Status field to enable or disable storm control.

Set the required threshold beyond which the switch will start dropping packets.

Click Apply.

**Figure 1: Configuring Storm Control**




| Port | Type | Unknown Unicast | | | Multicast | | | Broadcast | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Status | Rate (packets/sec) | | Status | Rate (packets/sec) | | Status | Rate (packets/sec) | |
| 1 | 1000Base-T | ☐ Enabled | 262143 | (500-262143) | ☐ Enabled | 262143 | (500-262143) | ☑ Enabled | 500 | (500-262143) |
| 2 | 1000Base-T | ☐ Enabled | 262143 | (500-262143) | ☐ Enabled | 262143 | (500-262143) | ☑ Enabled | 500 | (500-262143) |
| 3 | 1000Base-T | ☑ Enabled | 500 | (500-262143) | ☐ Enabled | 262143 | (500-262143) | ☐ Enabled | 500 | (500-262143) |
| 4 | 1000Base-T | ☐ Enabled | 262143 | (500-262143) | ☐ Enabled | 262143 | (500-262143) | ☑ Enabled | 500 | (500-262143) |
| 5 | 1000Base-T | ☐ Enabled | 262143 | (500-262143) | ☐ Enabled | 262143 | (500-262143) | ☑ Enabled | 500 | (500-262143) |
| 6 | 1000Base-T | ☐ Enabled | 262143 | (500-262143) | ☐ Enabled | 262143 | (500-262143) | ☑ Enabled | 550 | (500-262143) |
| 7 | 1000Base-T | ☐ Enabled | 262143 | (500-262143) | ☐ Enabled | 262143 | (500-262143) | ☑ Enabled | 500 | (500-262143) |
| 8 | 1000Base-T | ☐ Enabled | 262143 | (500-262143) | ☐ Enabled | 262143 | (500-262143) | ☑ Enabled | 500 | (500-262143) |
| 9 | 1000Base-T | ☐ Enabled | 262143 | (500-262143) | ☐ Enabled | 262143 | (500-262143) | ☑ Enabled | 500 | (500-262143) |
| 10 | 1000Base-T | ☐ Enabled | 262143 | (500-262143) | ☐ Enabled | 262143 | (500-262143) | ☑ Enabled | 500 | (500-262143) |

# 11 CLASS OF SERVICE

Class of Service (CoS) allows you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with eight priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, and configure the mapping of frame priority tags to the switch's priority queues.

This chapter describes the following basic topics:

- Layer 2 Queue Settings – Configures each queue, including the default priority, queue mode, and queue weight, and mapping of packets to queues based on CoS tags.
- Layer 3/4 Priority Settings – Maps TCP ports, IP precedence tags, or IP DSCP tags to class of service values.

## LAYER 2 QUEUE SETTINGS

This section describes how to configure the default priority for untagged frames, set the queue mode, set the weights assigned to each queue, and map class of service tags to queues.

### Setting the Default Priority for Interfaces

Use the Traffic > Priority > Default Priority page to specify the default port priority for each interface on the switch. All untagged packets entering the switch are tagged with the specified default port priority, and then sorted into the appropriate priority queue at the output port.

#### CLI REFERENCES

- "switchport priority default" on page 931

#### COMMAND USAGE

- This switch provides eight priority queues for each port. It uses Weighted Round Robin to prevent head-of-queue blockage, but can be configured to process each queue in strict order, or use a combination of strict and weighted queueing.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- If the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.

### PARAMETERS

These parameters are displayed in the web interface:

- **Interface** – Displays a list of ports or trunks.

- **CoS** – The priority that is assigned to untagged frames received on the specified interface. (Range: 0-7; Default: 0)

### WEB INTERFACE

To configure the queue mode:

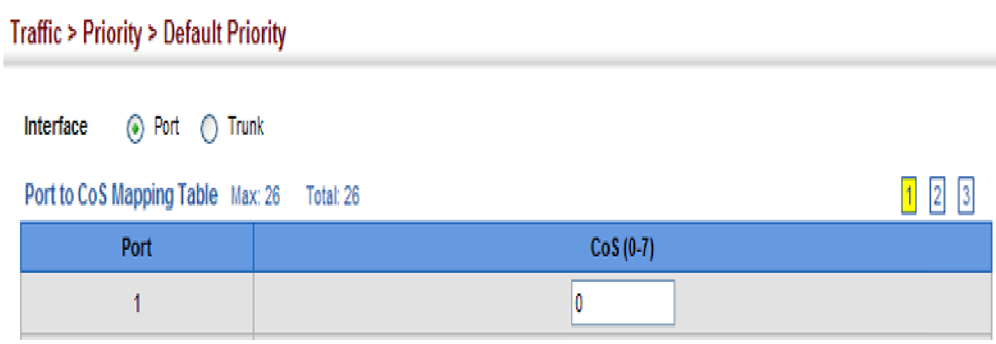
1. Click Traffic, Priority, Default Priority.

2. Select the interface type to display (Port or Trunk).

3. Modify the default priority for any interface.

4. Click Apply.

**Figure 1: Setting the Default Port Priority**




## Selecting the Queue Mode

Use the Traffic > Priority > Queue page to set the queue mode for the egress queues on any interface. The switch can be set to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before the lower priority queues are serviced, or Weighted Round-Robin (WRR) queuing which specifies a scheduling weight for each queue. It can also be configured to use a combination of strict and weighted queuing.

### CLI REFERENCES

- "queue mode" on page 929
- "show queue mode" on page 932

### COMMAND USAGE

- Strict priority requires all traffic in a higher priority queue to be processed before lower priority queues are serviced.

- WRR queuing specifies a relative weight for 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.

- If "Strict and WRR" mode is selected, a combination of strict service is used for the high priority queues and weighted service for the remaining queues. The queues assigned to use strict priority should be specified using the Strict Mode field parameter.

- A weight can be assigned to each of the weighted queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue is polled for service, and subsequently affects the response time for software applications assigned a specific priority value.

  Service time is shared at the egress ports by defining scheduling weights for WRR, or one of the queuing modes that use a combination of strict and weighted queuing.

### PARAMETERS

These parameters are displayed in the web interface:

- **Interface** – Displays a list of ports or trunks.

- **Queue Mode**

  - **Strict** – Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues. This ensures that the highest priority packets are always serviced first, ahead of all other traffic.

  - **WRR** – Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights, and servicing each queue in a round-robin fashion. This is the default selection.

  - **Strict and WRR** – Uses strict priority on the high-priority queues and WRR on the remaining queues.

- **Queue ID** – The ID of the priority queue. (Range: 0-7)

- **Strict Mode** – If "Strict and WRR" is selected, then a combination of strict service is used for the high priority queues and weighted service for the remaining queues. Use this parameter to specify the queues assigned to use strict priority. (Default: Disabled)

- **Weight** – Sets a weight for each queue which is used by the WRR scheduler. (Range: 1-15; Default: Weights 1, 2, 4, 6, 8, 10, 12, 14 are assigned to queues 0 - 7 respectively)

### WEB INTERFACE

To configure the queue mode:

1. Click Traffic, Priority, Queue.

2. Select the interface type to display (Port or Trunk).

3. Set the queue mode.

4. If any of the weighted queue modes is selected, the queue weight can be modified if required.

5. If any of the queue modes that use a combination of strict and weighted queueing are selected, the queues which are serviced first must be specified by enabling strict mode parameter in the table.

6. Click Apply.

**Figure 2: Setting the Queue Mode** (Strict)

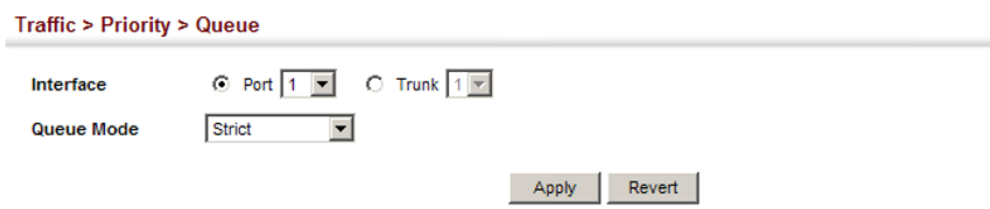



**Figure 3: Setting the Queue Mode** (WRR)

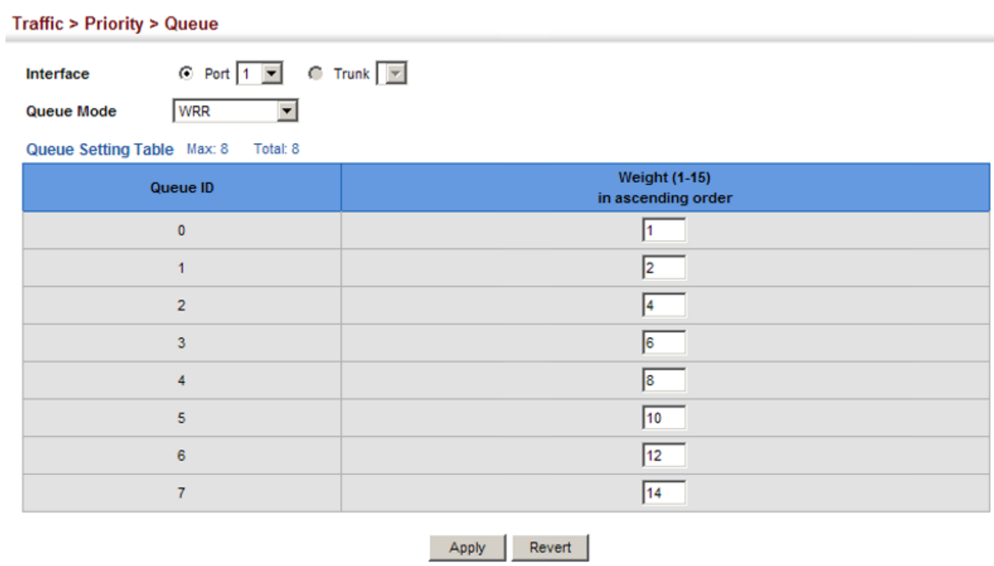
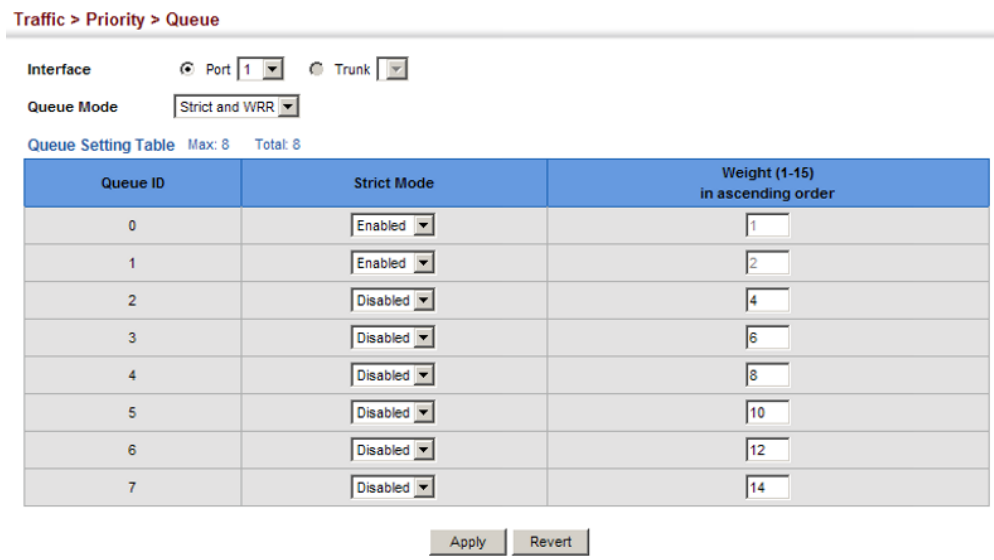


**Figure 4: Setting the Queue Mode** (Strict and WRR)




## Mapping CoS Values to Egress Queues

Use the Traffic > Priority > CoS to Queue page to specify the hardware output queues to use for Class of Service (CoS) priority tagged traffic.

The switch processes Class of Service (CoS) priority tagged traffic by using eight priority queues for each port, with service schedules based on strict priority, Weighted Round-Robin (WRR), or a combination of strict and weighted queuing. Up to eight separate traffic priorities are defined in IEEE 802.1p. Default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

**Table 1: IEEE 802.1p Egress Queue Priority Mapping**

| **Priority** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| **Queue** | 2 | 0 | 1 | 3 | 4 | 5 | 6 | 7 |

The priority levels recommended in the IEEE 802.1p standard for various network applications are shown in Table 2. However, priority levels can be mapped to the switch's output queues in any way that benefits application traffic for the network.

**Table 2: CoS Priority Levels**

| Priority Level | Traffic Type |
|---|---|
| 1 | Background |
| 2 | (Spare) |
| 0 (default) | Best Effort |
| 3 | Excellent Effort |
| 4 | Controlled Load |
| 5 | Video, less than 100 milliseconds latency and jitter |
| 6 | Voice, less than 10 milliseconds latency and jitter |
| 7 | Network Control |

### CLI REFERENCES


- "queue cos-map" on page 928
- "show queue cos-map" on page 932


### COMMAND USAGE

- Egress packets are placed into the hardware queues according to the mapping defined by this command.
- The specified mapping applies to all interfaces.

### PARAMETERS

These parameters are displayed:

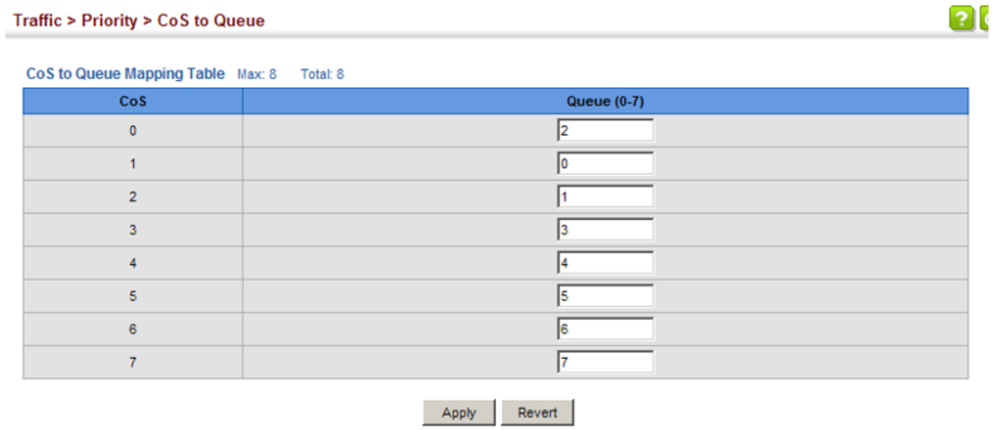
- **Priority** – CoS value. (Range: 0-7, where 7 is the highest priority)
- **Queue** – Output queue buffer. (Range: 0-7, where 7 is the highest CoS priority queue)

### WEB INTERFACE

To specify which of the output queues to use for CoS priority tagged traffic:

1. Click Traffic, Priority, CoS to Queue.
2. Assign priorities to the output queues.
3. Click Apply.

**Figure 5: Mapping CoS Values to Egress Queues**




## LAYER 3/4 PRIORITY SETTINGS

**Mapping Layer 3/4 Priorities to CoS Values**

The switch supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic priorities can be specified in the IP header of a frame, using the priority bits in the Type of Service (ToS) octet, or the number of the TCP/UDP port. If priority bits are used, the ToS octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

Because different priority information may be contained in the traffic, this switch maps priority values to the output queues in the following manner:

- The precedence for priority mapping is IP Port Priority, IP Precedence or DSCP Priority, and then Default Port Priority.
- IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.

### Mapping DSCP Priority

Use the Traffic > Priority > IP DSCP to CoS page to map IP DSCP priorities found in ingress packets to CoS values for internal priority processing.

#### CLI REFERENCES

- "map ip dscp (Global Configuration)" on page 934
- "map ip dscp (Interface Configuration)" on page 935
- "show map ip dscp" on page 938

#### COMMAND USAGE

- The DSCP is six bits wide, allowing coding for up to 64 different forwarding behaviors. The DSCP retains backward compatibility with the three precedence bits so that non-DSCP compliant devices will not conflict with the DSCP mapping.

Based on network policies, different kinds of traffic can be marked for different kinds of forwarding.

- 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 eight hardware priority queues. The default mapping is defined in the following table. Note that all the DSCP values that are not specified are mapped to CoS value 0.

**Table 3: 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 |

**Note:** IP DSCP settings apply to all interfaces.

## Parameters

These parameters are displayed:

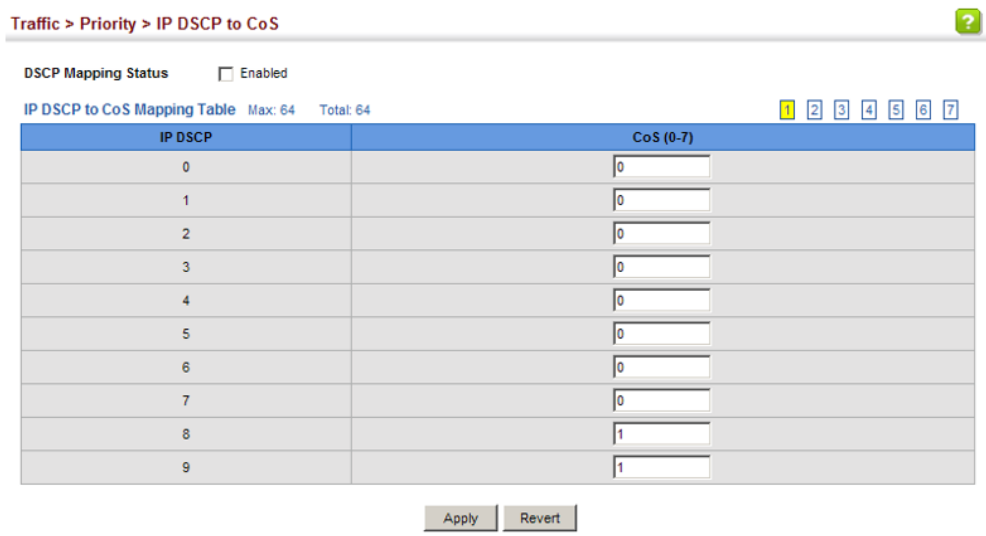
- **DSCP Mapping Status** – Enables or disables the use of IP DSCP priorities and the mapping of these priority values to CoS values. (Default: Disabled)
- **IP DSCP** – 8-bit DSCP value. (Range: 0-63)
- **CoS** – Class-of-Service value (Range: 0-7)

## Web Interface

To set the IP DSCP to CoS priority map:

1. Click Traffic, Priority, IP DSCP to CoS.
2. Locate an entry from the DSCP table, and enter a value in the CoS field.
3. Click Apply.

**Figure 6: Mapping IP DSCP Priority Values**




## Mapping IP Precedence

Use the Traffic > Priority > IP Precedence to CoS page to map IP Precedence priorities found in ingress packets to CoS values for internal priority processing.

### CLI REFERENCES

- "map ip precedence (Global Configuration)" on page 935
- "map ip precedence (Interface Configuration)" on page 937
- "show map ip precedence" on page 939

### COMMAND USAGE

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.

**Table 4: Usage of ToS Bits**

| Priority Level | Traffic Type |
|---|---|
| 0 | Routine |
| 1 | Priority |
| 2 | Immediate |
| 3 | Flash |
| 4 | Flash Override |
| 5 | Critical |
| 6 | Internetwork Control |
| 7 | Network Control |

**NOTE:** IP Precedence settings apply to all interfaces.

### PARAMETERS

These parameters are displayed:

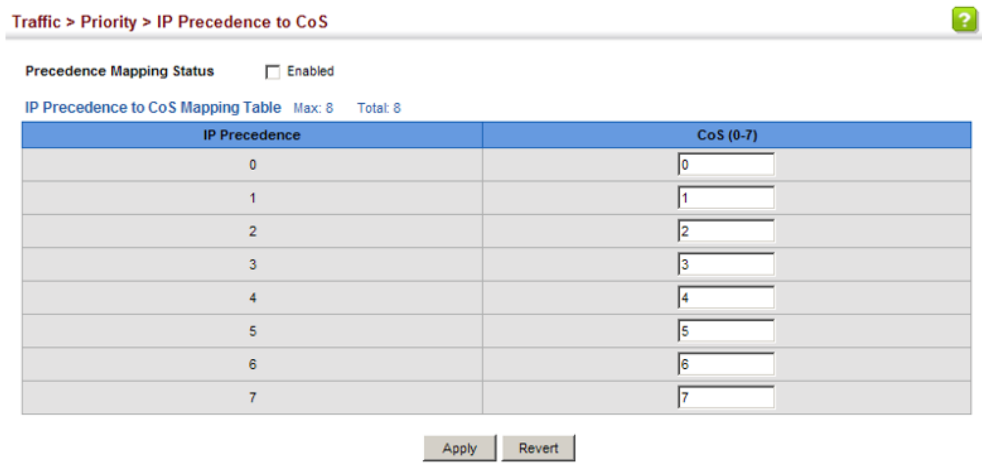
- **IP Precedence Mapping Status** – Enables or disables the use of IP Precedence priorities and the mapping of these priority values to CoS values. (Default: Disabled)
- **IP Precedence** – 3-bit precedence value. (Range: 0-7)
- **CoS** – Class-of-Service value (Range: 0-7)

### WEB INTERFACE

To set the IP Precedence to CoS priority map:

1. Click Traffic, Priority, IP Precedence to CoS.
2. Locate an entry from the IP Precedence table, and enter a value in the CoS field.
3. Click Apply.

**Figure 7: Mapping IP Precedence Priority Values**




## Mapping IP Port Priority

Use the Traffic > Priority > IP Port to CoS page to map network applications designated by a TCP/UDP destination port number in the frame header to CoS values for internal processing.

### CLI REFERENCES

- "map ip port (Global Configuration)" on page 934
- "map ip port (Interface Configuration)" on page 936
- "show map ip port" on page 938

### COMMAND USAGE

- This mapping table is only used if the protocol type of the arriving packet is TCP or UDP. Some of the more common TCP service ports include: HTTP: 80, FTP: 21, Telnet: 23 and POP3: 110.

- No default mapping is defined for ingress TCP/UDP port types.

**NOTE:** IP Port settings apply to all interfaces.

### PARAMETERS

These parameters are displayed in the web interface:

- **IP Port Mapping Status** – Enables or disables the use of TCP/UDP destination port numbers priorities and the mapping of these priority values to CoS values. (Default: Disabled)

- **TCP/UDP Port** – 16-bit TCP/UDP destination port number. (Range: 0-65535)

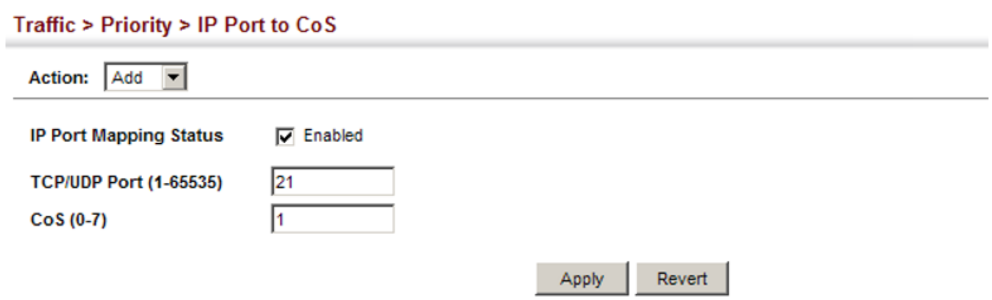
- **CoS** – Class-of-Service value (Range: 0-7)

### WEB INTERFACE

To set the TCP/UDP port number to CoS priority map:

1. Click Traffic, Priority, IP Port to CoS.
2. Select Add from the Action list.
3. Set the CoS priority for any TCP or UDP port.
4. Click Apply.

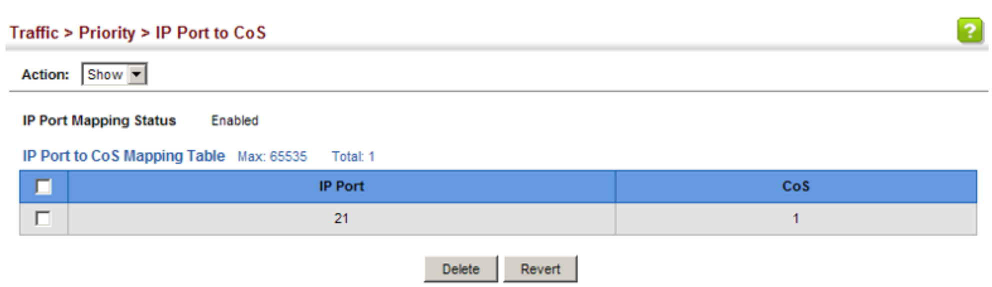
**Figure 8: Mapping IP Port Number Priority Values**




To show the TCP/UDP port number to CoS priority map:

1. Click Traffic, Priority, IP Port to DSCP.
2. Select Show from the Action list.

**Figure 9: Showing IP Port Number Priority Map**



# 12 QUALITY OF SERVICE

This chapter describes the following tasks required to apply QoS policies:

Class Map – Creates a map which identifies a specific class of traffic.

Policy Map – Sets the boundary parameters used for monitoring inbound traffic, and the action to take for conforming and non-conforming traffic.

Binding to a Port – Applies a policy map to an ingress port.

## OVERVIEW

The commands described in this section are used to configure Quality of Service (QoS) classification criteria and service policies. Differentiated Services (DiffServ) provides policy-based management mechanisms used for prioritizing network resources to meet the requirements of specific traffic types on a per hop basis. Each packet is classified upon entry into the network based on access lists, IP Precedence, DSCP values, or VLAN lists. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet. Based on configured network policies, different kinds of traffic can be marked for different kinds of forwarding.

All switches or routers that access the Internet rely on class information to provide the same forwarding treatment to packets in the same class. Class information can be assigned by end hosts, or switches or routers along the path. Priority can then be assigned based on a general policy, or a detailed examination of the packet. However, note that detailed examination of packets should take place close to the network edge so that core switches and routers are not overloaded.

Switches and routers along the path can use class information to prioritize the resources allocated to different traffic classes. The manner in which an individual device handles traffic in the DiffServ architecture is called per-hop behavior. All devices along a path should be configured in a consistent manner to construct a consistent end-to-end QoS solution.

**NOTE:** You can configure up to 16 rules per class map. You can also include multiple classes in a policy map.

**NOTE:** You should create a class map before creating a policy map. Otherwise, you will not be able to select a class nap from the policy rule settings screen (see page 221).

### COMMAND USAGE

To create a service policy for a specific category or ingress traffic, follow these steps:

1. Use the Configure Class (Add) page to designate a class name for a specific category of traffic.

2. Use the Configure Class (Add Rule) page to edit the rules for each class which specify a type of traffic based on an access list, a DSCP or IP Precedence value, or a VLAN.

3. Use the Configure Policy (Add) page to designate a policy name for a specific manner in which ingress traffic will be handled.

4. Use the Configure Policy (Add Rule) page to add one or more classes to the policy map. Assign policy rules to each class by "setting" the QoS value (CoS or PHB) to be assigned to the matching traffic class. The policy rule can also be configured to monitor the maximum throughput and burst rate. Then specify the action to take for conforming traffic, or the action to take for a policy violation.

5. Use the Configure Interface page to assign a policy map to a specific interface.

## CONFIGURING A CLASS MAP

A class map is used for matching packets to a specified class. Use the Traffic > DiffServ (Configure Class) page to configure a class map.

### CLI REFERENCES

- "Quality of Service Commands" on page 941

### COMMAND USAGE

- The class map is used with a policy map (page 221) to create a service policy (page 230) for a specific interface that defines packet classification, service tagging, and bandwidth policing. Note that one or more class maps can be assigned to a policy map.

- Up to 32 class maps can be configured.

### PARAMETERS

These parameters are displayed in the web interface:

*Add*

- **Class Name** – Name of the class map. (Range: 1-16 characters)

- **Type** – Only one match command is permitted per class map, so the match-any field refers to the criteria specified by the lone match command.

- **Description** – A brief description of a class map. (Range: 1-64 characters)

*Add Rule*

- **Class Name** – Name of the class map.

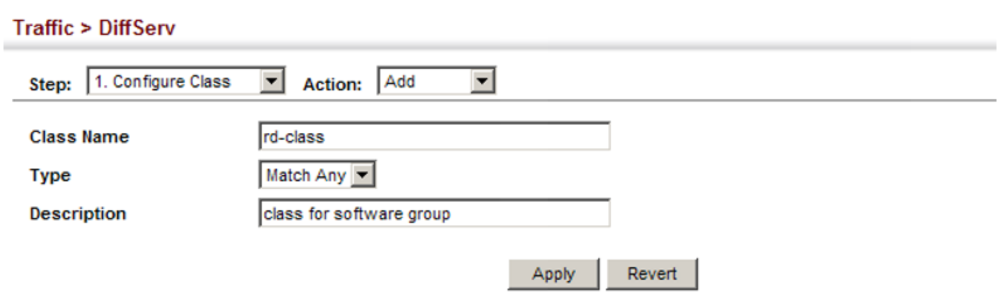
- **Type** – Only one match command is permitted per class map, so the match-any field refers to the criteria specified by the lone match command.
- **ACL** – Name of an access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs.
- **IP DSCP** – A DSCP value. (Range: 0-63)
- **IP Precedence** – An IP Precedence value. (Range: 0-7)
- **IPv6 DSCP** – A DSCP value contained in an IPv6 packet. (Range: 0-63)
- **VLAN ID** – A VLAN. (Range:1-4093)

### WEB INTERFACE

To configure a class map:

1. Click Traffic, DiffServ.
2. Select Configure Class from the Step list.
3. Select Add from the Action list.
4. Enter a class name.
5. Enter a description.
6. Click Apply.

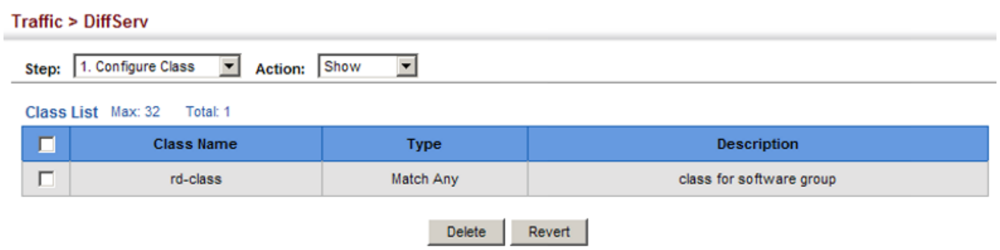
**Figure 1: Configuring a Class Map**



To show the configured class maps:

1. Click Traffic, DiffServ.
2. Select Configure Class from the Step list.
3. Select Show from the Action list.

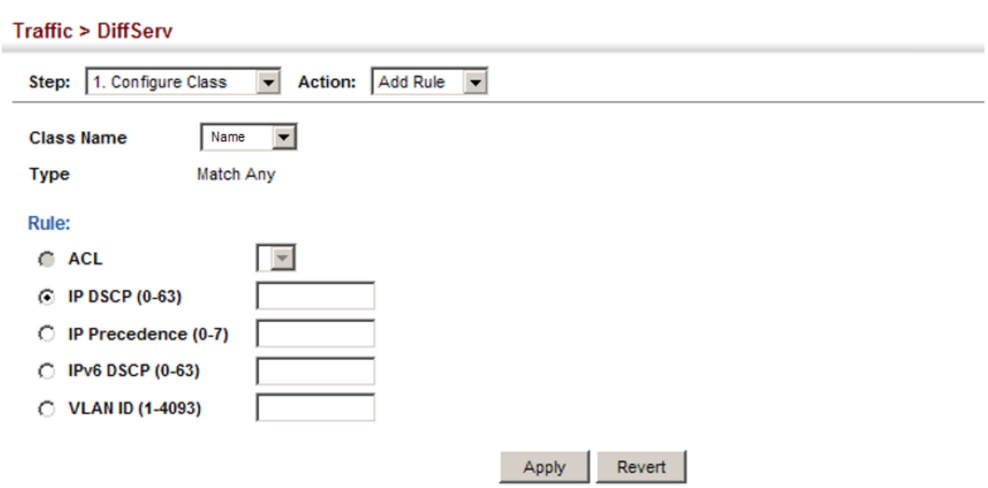
**Figure 2: Showing Class Maps**




To edit the rules for a class map:

1. Click Traffic, DiffServ.
2. Select Configure Class from the Step list.
3. Select Add Rule from the Action list.
4. Select the name of a class map.
5. Specify type of traffic for this class based on an access list, a DSCP or IP Precedence value, or a VLAN. You can specify up to 16 items to match when assigning ingress traffic to a class map.
6. Click Apply.

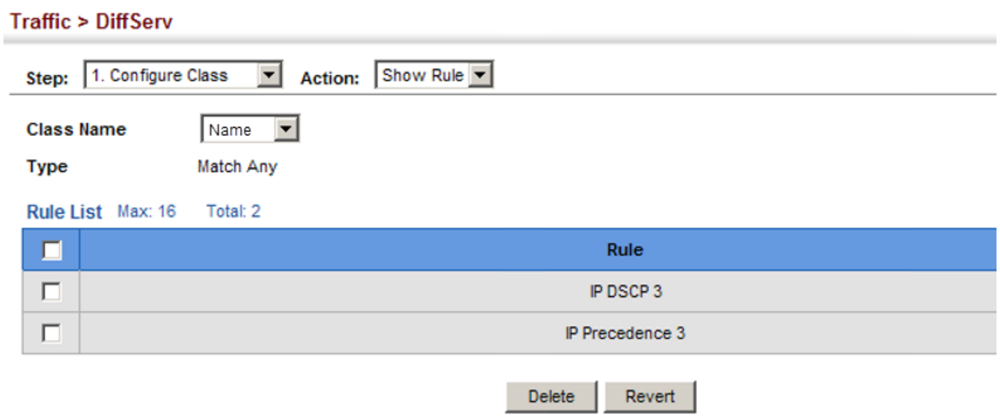
**Figure 3: Adding Rules to a Class Map**



To show the rules for a class map:

1. Click Traffic, DiffServ.
2. Select Configure Class from the Step list.
3. Select Show Rule from the Action list.

**Figure 4: Showing the Rules for a Class Map**




## CREATING QOS POLICIES

Use the Traffic > DiffServ (Configure Policy) page to create a policy map that can be attached to multiple interfaces. A policy map is used to group one or more class map statements (page 218), modify service tagging, and enforce bandwidth policing. A policy map can then be bound by a service policy to one or more interfaces (page 230).

Configuring QoS policies requires several steps. A class map must first be configured which indicates how to match the inbound packets according to an access list, a DSCP or IP Precedence value, or a member of specific VLAN. A policy map is then configured which indicates the boundary parameters used for monitoring inbound traffic, and the action to take for conforming and non-conforming traffic. A policy map may contain one or more classes based on previously defined class maps.

The class of service or per-hop behavior (i.e., the priority used for internal queue processing) can be assigned to matching packets. In addition, the flow rate of inbound traffic can be monitored and the response to conforming and non-conforming traffic based by one of three distinct policing methods as described below.

**Police Flow Meter** – Defines the committed information rate (maximum throughput), committed burst size (burst rate), and the action to take for conforming and non-conforming traffic.

Policing is based on a token bucket, where bucket depth (that is, the maximum burst before the bucket overflows) is specified by the “burst” field (BC), and the average rate tokens are removed from the bucket is specified by the “rate” option (CIR). Action may be taken for traffic conforming to the maximum throughput, or exceeding the maximum throughput.

**srTCM Police Meter** – Defines an enforcer for classified traffic based on a single rate three color meter scheme defined in RFC 2697. This metering policy monitors a traffic stream and processes its packets according to the committed information rate (CIR, or maximum throughput), committed burst size (BC, or burst rate), and excess burst size (BE). Action may taken for traffic conforming to the maximum throughput, exceeding the maximum throughput, or exceeding the excess burst size.

- The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. In addition to the actions defined by this command to transmit, remark the DSCP service value, or drop a packet, the switch will also mark the two color bits which are used to prioritize service to packets of different colors as described below. A packet is marked green if it doesn't exceed the committed information rate and committed burst size, yellow if it does exceed the committed information rate and committed burst size, but not the excess burst size, and red otherwise.

- The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The marker (re)colors an IP packet according to the results of the meter. The color is coded in the DS field [RFC 2474] of the packet.

- The behavior of the meter is specified in terms of its mode and two token buckets, C and E, which both share the common rate CIR. The maximum size of the token bucket C is BC and the maximum size of the token bucket E is BE.

  The token buckets C and E are initially full, that is, the token count Tc(0) = BC and the token count Te(0) = BE. Thereafter, the token counts Tc and Te are updated CIR times per second as follows:

  - If Tc is less than BC, Tc is incremented by one, else
  - if Te is less then BE, Te is incremented by one, else
  - neither Tc nor Te is incremented.

  When a packet of size B bytes arrives at time t, the following happens if srTCM is configured to operate in Color-Blind mode:

  - If Tc(t)-B ≥ 0, the packet is green and Tc is decremented by B down to the minimum value of 0, else
  - if Te(t)-B ≥ 0, the packets is yellow and Te is decremented by B down to the minimum value of 0,
  - else the packet is red and neither Tc nor Te is decremented.

  When a packet of size B bytes arrives at time t, the following happens if srTCM is configured to operate in Color-Aware mode:

- ◆ If the packet has been precolored as green and Tc(t)-B ≥ 0, the packet is green and Tc is decremented by B down to the minimum value of 0, else
- ◆ If the packet has been precolored as yellow or green and if Te(t)-B ≥ 0, the packets is yellow and Te is decremented by B down to the minimum value of 0, else
- ◆ the packet is red and neither Tc nor Te is decremented.

The metering policy guarantees a deterministic behavior where the volume of green packets is never smaller than what has been determined by the CIR and BC, that is, tokens of a given color are always spent on packets of that color. Refer to RFC 2697 for more information on other aspects of srTCM.

**trTCM Police Meter** – Defines an enforcer for classified traffic based on a two rate three color meter scheme defined in RFC 2698. This metering policy monitors a traffic stream and processes its packets according to the committed information rate (CIR, or maximum throughput), peak information rate (PIR), and their associated burst sizes – committed burst size (BC, or burst rate), and peak burst size (BP). Action may taken for traffic conforming to the maximum throughput, exceeding the maximum throughput, or exceeding the peak burst size.

- ■The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. In addition to the actions defined by this command to transmit, remark the DSCP service value, or drop a packet, the switch will also mark the two color bits which are used to prioritize service to packets of different colors as described below. A packet is marked red if it exceeds the PIR. Otherwise it is marked either yellow or green depending on whether it exceeds or doesn't exceed the CIR.

  The trTCM is useful for ingress policing of a service, where a peak rate needs to be enforced separately from a committed rate.

- ■The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The marker (re)colors an IP packet according to the results of the meter. The color is coded in the DS field [RFC 2474] of the packet.

- ■The behavior of the meter is specified in terms of its mode and two token buckets, P and C, which are based on the rates PIR and CIR, respectively. The maximum size of the token bucket P is BP and the maximum size of the token bucket C is BC.

  The token buckets P and C are initially (at time 0) full, that is, the token count Tp(0) = BP and the token count Tc(0) = BC. Thereafter, the token count Tp is incremented by one PIR times per second up to BP and the token count Tc is incremented by one CIR times per second up to BC.

  When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in Color-Blind mode:

  - ◆ If Tp(t)-B < 0, the packet is red, else

- if Tc(t)-B < 0, the packet is yellow and Tp is decremented by B, else
- the packet is green and both Tp and Tc are decremented by B.

When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in Color-Aware mode:

- If the packet has been precolored as red or if Tp(t)-B < 0, the packet is red, else
- if the packet has been precolored as yellow or if Tc(t)-B < 0, the packet is yellow and Tp is decremented by B, else
- the packet is green and both Tp and Tc are decremented by B.

■ The trTCM can be used to mark a IP packet stream in a service, where different, decreasing levels of assurances (either absolute or relative) are given to packets which are green, yellow, or red. Refer to RFC 2698 for more information on other aspects of trTCM.

### CLI REFERENCES

■ "Quality of Service Commands" on page 941

### COMMAND USAGE

■ A policy map can contain 128 class statements that can be applied to the same interface (page 230). Up to 26 policy maps can be configured for ingress ports.

■ After using the policy map to define packet classification, service tagging, and bandwidth policing, it must be assigned to a specific interface by a service policy (page 230) to take effect.

### PARAMETERS

These parameters are displayed in the web interface:

*Add*

■ **Policy Name** – Name of policy map. (Range: 1-16 characters)

■ **Description** – A brief description of a policy map. (Range: 1-256 characters)

*Add Rule*

■ **Policy Name** – Name of policy map.

■ **Class Name** – Name of a class map that defines a traffic classification upon which a policy can act.

■ **Action** – Configures the service provided to ingress traffic. Packets matching the rule settings for a class map can be remarked as follows:

- **Set CoS** – Sets a priority bits in the VLAN tag for matching packets. (Range: 0-7)

- **Set IP DSCP** – Configures the service provided to ingress traffic by setting an IP DSCP value for a matching packet (as specified in rule settings for a class map. (Range: 0-63)
- **Set IP Precedence** – Configures the service provided to ingress traffic by setting an IP Precedence value for a matching packet (as specified in rule settings for a class map. (Range: 0-63)

■ **Meter** – Check this to define the maximum throughput, burst rate, and the action that results from a policy violation.

■ **Meter Mode** – Selects one of the following policing methods.

- **Flow** (Police Flow) – Defines the committed information rate (CIR, or maximum throughput), committed burst size (BC, or burst rate), and the action to take for conforming and non-conforming traffic. Policing is based on a token bucket, where bucket depth (that is, the maximum burst before the bucket overflows) is specified by the “burst” field, and the average rate tokens are removed from the bucket is by specified by the “rate” option.
  - **Committed Information Rate** (CIR) – Rate in kilobits per second. (Range: 1-1000000 kbps or maximum port speed, whichever is lower)

    The rate cannot exceed the configured interface speed.
  - **Committed Burst Size** (BC) – Burst in bytes. (Range: 64-524288 bytes)

    The burst size cannot exceed 16 Mbytes.
  - **Conform** – Specifies whether that traffic conforming to the maximum rate (CIR) will be transmitted without any change to the DSCP service level, or if the DSCP service level will be modified.
    - **Transmit** – Transmits in-conformance traffic without any change to the DSCP service level.
  - **Violate** – Specifies whether the traffic that exceeds the maximum rate (CIR) will be dropped or the DSCP service level will be reduced.
    - **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63)
    - **Drop** – Drops out of conformance traffic.
- **srTCM** (Police Meter) – Defines the committed information rate (CIR, or maximum throughput), committed burst size (BC, or burst rate) and excess burst size (BE), and the action to take for traffic conforming to the maximum throughput, exceeding the maximum throughput but within the excess burst size, or exceeding the excess burst size. In addition to the actions defined by this command to transmit, remark the DSCP service value, or drop a packet, the switch will also mark the two color bits used to prioritize service to packets of different colors.

  The color modes include “Color-Blind” which assumes that the packet stream is uncolored, and “Color-Aware” which assumes that the incoming packets are pre-colored. The functional differences between these modes is described at the beginning of this section under “srTCM Police Meter.”

- **Committed Information Rate** (CIR) – Rate in kilobits per second. (Range: 1-1000000 kbps or maximum port speed, whichever is lower)

  The rate cannot exceed the configured interface speed.

- **Committed Burst Size** (BC) – Burst in bytes. (Range: 64-524288 bytes)

  The burst size cannot exceed 16 Mbytes.

- **Exceeded Burst Size** (BE) – Burst in excess of committed burst size. (Range: 64-524288 bytes)

  The burst size cannot exceed 16 Mbytes.

- **Conform** – Specifies whether that traffic conforming to the maximum rate (CIR) will be transmitted without any change to the DSCP service level, or if the DSCP service level will be modified.

  - **Transmit** – Transmits in-conformance traffic without any change to the DSCP service level.

- **Exceed** – Specifies whether traffic that exceeds the maximum rate (CIR) but is within the excess burst size (BE) will be dropped or the DSCP service level will be reduced.

  - **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63)

  - **Drop** – Drops out of conformance traffic.

- **Violate** – Specifies whether the traffic that exceeds the excess burst size (BE) will be dropped or the DSCP service level will be reduced.

  - **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63)

  - **Drop** – Drops out of conformance traffic.

◆ **trTCM** (Police Meter) – Defines the committed information rate (CIR, or maximum throughput), peak information rate (PIR), and their associated burst sizes – committed burst size (BC, or burst rate) and peak burst size (BP), and the action to take for traffic conforming to the maximum throughput, exceeding the maximum throughput but within the peak information rate, or exceeding the peak information rate. In addition to the actions defined by this command to transmit, remark the DSCP service value, or drop a packet, the switch will also mark the two color bits used to prioritize service to packets of different colors.

The color modes include “Color-Blind” which assumes that the packet stream is uncolored, and “Color-Aware” which assumes that the incoming packets are pre-colored. The functional differences between these modes is described at the beginning of this section under “trTCM Police Meter.”

- **Committed Information Rate** (CIR) – Rate in kilobits per second. (Range: 1-1000000 kbps or maximum port speed, whichever is lower)

  The rate cannot exceed the configured interface speed.

- **Peak Information Rate** (PIR) – Rate in kilobits per second. (Range: 1-1000000 kbps or maximum port speed, whichever is lower)

  The rate cannot exceed the configured interface speed.

- **Committed Burst Size** (BC) – Burst in bytes. (Range: 64-524288 bytes)

  The burst size cannot exceed 16 Mbytes.

- **Peak Burst Size** (BP) – Burst size in bytes. (Range: 64-524288 bytes)

  The burst size cannot exceed 16 Mbytes.

- **Conform** – Specifies whether that traffic conforming to the maximum rate (CIR) will be transmitted without any change to the DSCP service level, or if the DSCP service level will be modified.

  - **Transmit** – Transmits in-conformance traffic without any change to the DSCP service level.

- **Exceed** – Specifies whether traffic that exceeds the maximum rate (CIR) but is within the peak information rate (PIR) will be dropped or the DSCP service level will be reduced.

  - **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63).

  - **Drop** – Drops out of conformance traffic.

- **Violate** – Specifies whether the traffic that exceeds the peak information rate (PIR) will be dropped or the DSCP service level will be reduced.

  - **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63).

  - **Drop** – Drops out of conformance traffic.

**WEB INTERFACE**

To configure a policy map:

1. Click Traffic, DiffServ.

2. Select Configure Policy from the Step list.

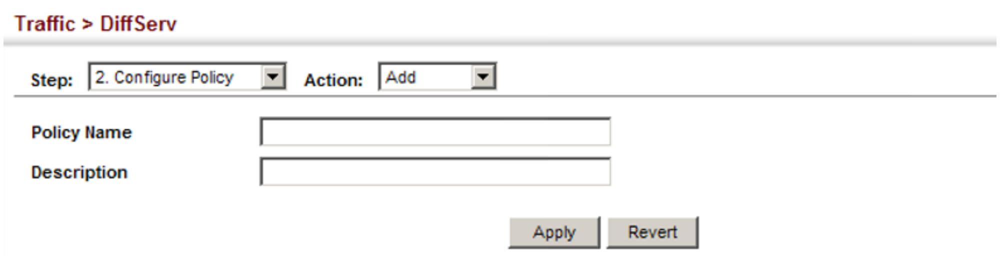
3. Select Add from the Action list.

4. Enter a policy name.

5. Enter a description.

6. Click Apply.

**Figure 5: Configuring a Policy Map**



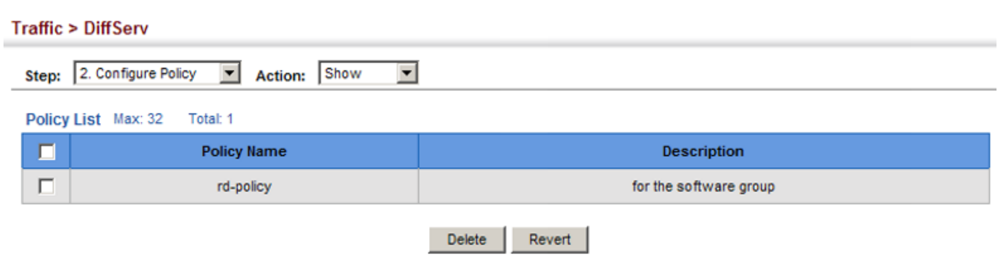

To show the configured policy maps:

1. Click Traffic, DiffServ.

2. Select Configure Policy from the Step list.

3. Select Show from the Action list.

**Figure 6: Showing Policy Maps**




To edit the rules for a policy map:

1. Click Traffic, DiffServ.

2. Select Configure Policy from the Step list.

3. Select Add Rule from the Action list.

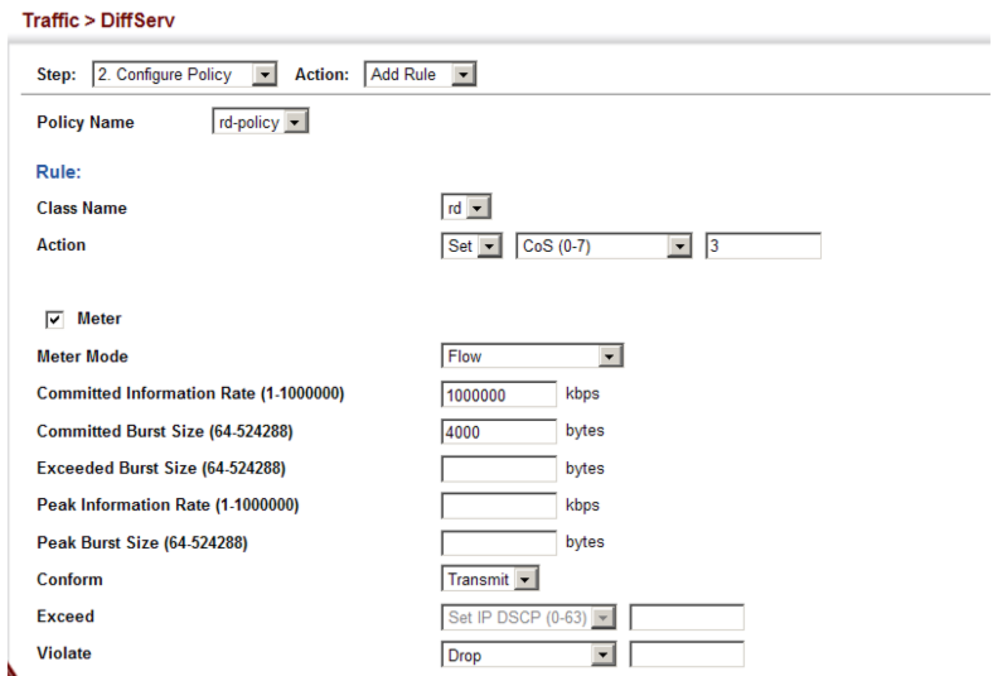
4. Select the name of a policy map.

5. Set the CoS or per-hop behavior for matching packets to specify the quality of service to be assigned to the matching traffic class. Use one of the metering options to define parameters such as the maximum throughput and burst rate. Then specify the action to take for conforming traffic, the action to tack for traffic in

excess of the maximum rate but within the peak information rate, or the action to take for a policy violation.

6. Click Apply.

**Figure 7: Adding Rules to a Policy Map**



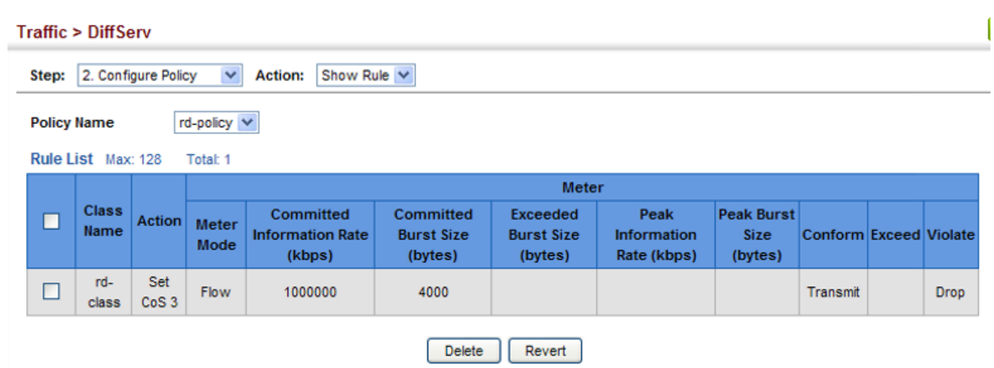

To show the rules for a policy map:

1. Click Traffic, DiffServ.

2. Select Configure Policy from the Step list.

3. Select Show Rule from the Action list.

**Figure 8: Showing the Rules for a Policy Map**



## ATTACHING A POLICY MAP TO A PORT

Use the Traffic > DiffServ (Configure Interface) page to bind a policy map to an ingress port.

### CLI REFERENCES

■ "Quality of Service Commands" on page 941

### COMMAND USAGE

■ First define a class map, define a policy map, and bind the service policy to the required interface.

■ Only one policy map can be bound to an interface.

■ The switch does not allow a policy map to be bound to an interface for egress traffic.

### PARAMETERS

These parameters are displayed in the web interface:

■ **Port** – Specifies a port.

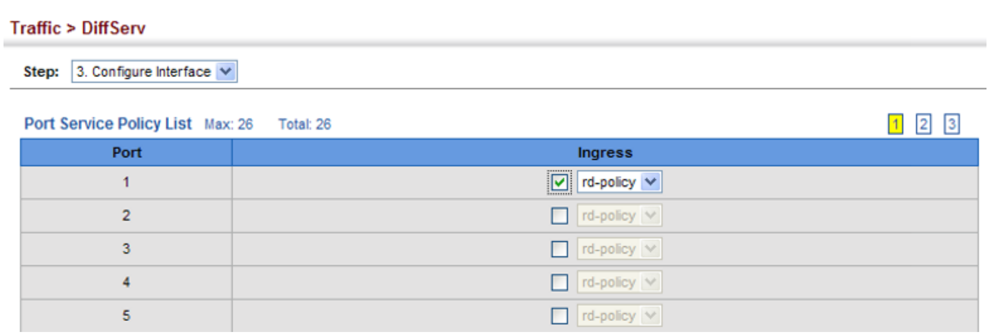
■ **Ingress** – Applies the selected rule to ingress traffic.

### WEB INTERFACE

To bind a policy map to a port:

1. Click Traffic, DiffServ.
2. Select Configure Interface from the Step list.
3. Check the box under the Ingress field to enable a policy map for a port.
4. Select a policy map from the scroll-down box.
5. Click Apply.

**Figure 9: Attaching a Policy Map to a Port**



# 13 VOIP TRAFFIC CONFIGURATION

This chapter covers the following topics:

- Global Settings page 231 – Enables VOIP globally, sets the Voice VLAN, and the aging time for attached ports.
- Telephony OUI List page 232 – Configures the list of phones to be treated as VOIP devices based on the specified Organization Unit Identifier (OUI).
- Port Settings page 234 – Configures the way in which a port is added to the Voice VLAN, the filtering of non-VoIP packets, the method of detecting VoIP traffic, and the priority assigned to voice traffic.

## OVERVIEW

When IP telephony is deployed in an enterprise network, it is recommended to isolate the Voice over IP (VoIP) network traffic from other data traffic. Traffic isolation can provide higher voice quality by preventing excessive packet delays, packet loss, and jitter. This is best achieved by assigning all VoIP traffic to a single Voice VLAN.

The use of a Voice VLAN has several advantages. It provides security by isolating the VoIP traffic from other data traffic. End-to-end QoS policies and high priority can be applied to VoIP VLAN traffic across the network, guaranteeing the bandwidth it needs. VLAN isolation also protects against disruptive broadcast and multicast traffic that can seriously affect voice quality.

The switch allows you to specify a Voice VLAN for the network and set a CoS priority for the VoIP traffic. The VoIP traffic can be detected on switch ports by using the source MAC address of packets, or by using LLDP (IEEE 802.1AB) to discover connected VoIP devices. When VoIP traffic is detected on a configured port, the switch automatically assigns the port as a tagged member the Voice VLAN. Alternatively, switch ports can be manually configured.

## CONFIGURING VOIP TRAFFIC

Use the Traffic > VoIP (Configure Global) page to configure the switch for VoIP traffic. First enable automatic detection of VoIP devices attached to the switch ports, then set the Voice VLAN ID for the network. The Voice VLAN aging time can also be set to remove a port from the Voice VLAN when VoIP traffic is no longer received on the port.

### CLI REFERENCES

- "Configuring Voice VLANs" on page 919

### Parameters

These parameters are displayed in the web interface:

- **Auto Detection Status** – Enables the automatic detection of VoIP traffic on switch ports. (Default: Disabled)
- **Voice VLAN** – Sets the Voice VLAN ID for the network. Only one Voice VLAN is supported and it must already be created on the switch. (Range: 1-4093)
- **Voice VLAN Aging Time** – The time after which a port is removed from the Voice VLAN when VoIP traffic is no longer received on the port. (Range: 5-43200 minutes; Default: 1440 minutes)

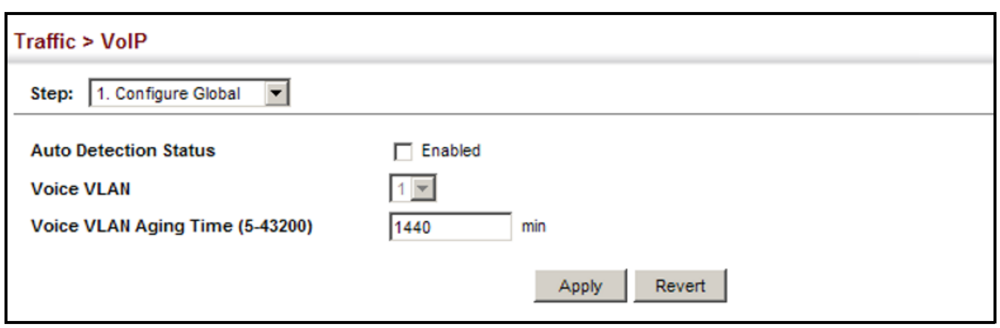
**Note:** The Voice VLAN ID cannot be modified when the global Auto Detection Status is enabled.

### Web Interface

To configure global settings for a Voice VLAN:

1. Click Traffic, VoIP.
2. Select Configure Global from the Step list.
3. Enable Auto Detection.
4. Specify the Voice VLAN ID.
5. Adjust the Voice VLAN Aging Time if required.
6. Click Apply.

**Figure 1: Configuring a Voice VLAN**




## Configuring Telephony OUI

VoIP devices attached to the switch can be identified by the manufacturer's Organizational Unique Identifier (OUI) in the source MAC address of received packets. OUI numbers are assigned to manufacturers and form the first three octets of device MAC addresses. The MAC OUI numbers for VoIP equipment can be configured on the switch so that traffic from these devices is recognized as VoIP. Use the Traffic > VoIP (Configure OUI) page to configure this feature.

### CLI REFERENCES

■ "Configuring Voice VLANs" on page 919

### PARAMETERS

These parameters are displayed in the web interface:

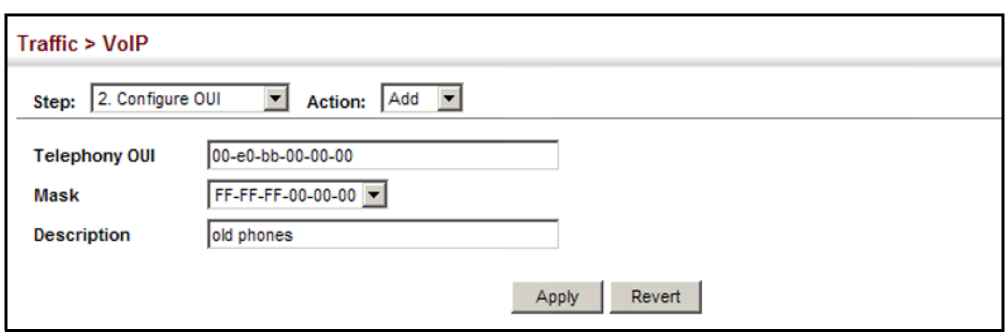
- **Telephony OUI** – Specifies a MAC address range to add to the list. Enter the MAC address in format 01-23-45-67-89-AB.
- **Mask** – Identifies a range of MAC addresses. Selecting a mask of FF-FF-FF-00-00-00 identifies all devices with the same OUI (the first three octets). Other masks restrict the MAC address range. Selecting FF-FF-FF-FF-FF-FF specifies a single MAC address. (Default: FF-FF-FF-00-00-00)
- **Description** – User-defined text that identifies the VoIP devices.

### WEB INTERFACE

To configure MAC OUI numbers for VoIP equipment:

1. Click Traffic, VoIP.
2. Select Configure OUI from the Step list.
3. Select Add from the Action list.
4. Enter a MAC address that specifies the OUI for VoIP devices in the network.
5. Select a mask from the pull-down list to define a MAC address range.
6. Enter a description for the devices.
7. Click Apply.

**Figure 2: Configuring an OUI Telephony List**



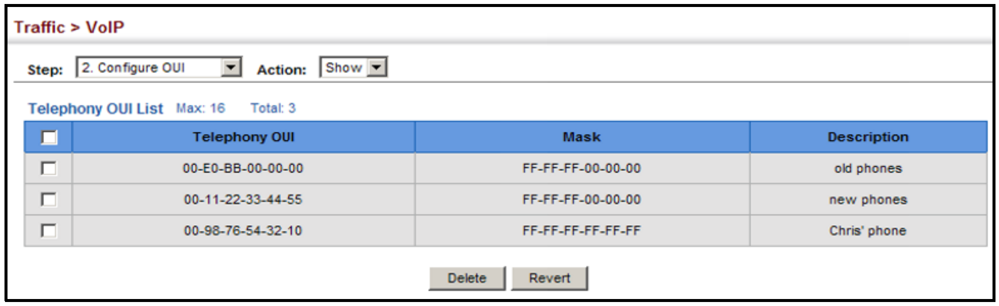

To show the MAC OUI numbers used for VoIP equipment:

1. Click Traffic, VoIP.

**2.** Select Configure OUI from the Step list.

**3.** Select Show from the Action list.

**Figure 3: Showing an OUI Telephony List**




## Configuring VoIP Traffic Ports

Use the Traffic > VoIP (Configure Interface) page to configure ports for VoIP traffic, you need to set the mode (Auto or Manual), specify the discovery method to use, and set the traffic priority. You can also enable security filtering to ensure that only VoIP traffic is forwarded on the Voice VLAN.

### CLI References

■ "Configuring Voice VLANs" on page 919

### Parameters

These parameters are displayed in the web interface:

■ **Mode** – Specifies if the port will be added to the Voice VLAN when VoIP traffic is detected. (Default: None)

- ◆ **None** – The Voice VLAN feature is disabled on the port. The port will not detect VoIP traffic or be added to the Voice VLAN.
- ◆ **Auto** – The port will be added as a tagged member to the Voice VLAN when VoIP traffic is detected on the port. You must select a method for detecting VoIP traffic, either OUI or 802.1ab (LLDP). When OUI is selected, be sure to configure the MAC address ranges in the Telephony OUI list.
- ◆ **Manual** – The Voice VLAN feature is enabled on the port, but the port must be manually added to the Voice VLAN.

■ **Security** – Enables security filtering that discards any non-VoIP packets received on the port that are tagged with the voice VLAN ID. VoIP traffic is identified by source MAC addresses configured in the Telephony OUI list, or through LLDP that discovers VoIP devices attached to the switch. Packets received from non-VoIP sources are dropped. (Default: Disabled)

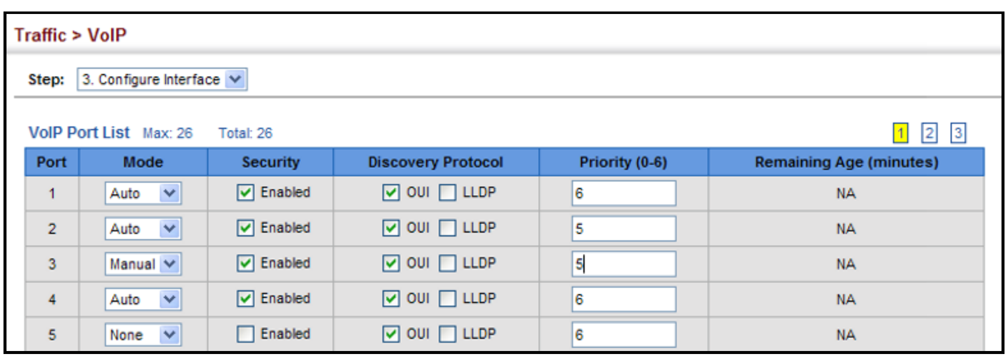
- **Discovery Protocol** – Selects a method to use for detecting VoIP traffic on the port. (Default: OUI)
  - **OUI** – Traffic from VoIP devices is detected by the Organizationally Unique Identifier (OUI) of the source MAC address. OUI numbers are assigned to manufacturers and form the first three octets of a device MAC address. MAC address OUI numbers must be configured in the Telephony OUI list so that the switch recognizes the traffic as being from a VoIP device.
  - **LLDP** – Uses LLDP (IEEE 802.1ab) to discover VoIP devices attached to the port. LLDP checks that the “telephone bit” in the system capability TLV is turned on. See "Link Layer Discovery Protocol" on page 330 for more information on LLDP.
- **Priority** – Defines a CoS priority for port traffic on the Voice VLAN. The priority of any received VoIP packet is overwritten with the new priority when the Voice VLAN feature is active for the port. (Range: 0-6; Default: 6)
- **Remaining Age** – Number of minutes before this entry is aged out.

### WEB INTERFACE

To configure VoIP traffic settings for a port:

1. Click Traffic, VoIP.
2. Select Configure Interface from the Step list.
3. Configure any required changes to the VoIP settings each port.
4. Click Apply.

**Figure 4: Configuring Port Settings for a Voice VLAN**



# 14 SECURITY MEASURES

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

- AAA – Use local or remote authentication to configure access rights, specify authentication servers, configure remote authentication and accounting.
- User Accounts – Manually configure access rights on the switch for specified users.
- Web Authentication – Allows stations to authenticate and access the network in situations where 802.1X or Network Access authentication methods are infeasible or impractical.
- Network Access - Configure MAC authentication and dynamic VLAN assignment.
- HTTPS – Provide a secure web connection.
- SSH – Provide a secure shell (for secure Telnet access).
- ACL – Access Control Lists provide packet filtering for IP frames (based on address, protocol, Layer 4 protocol port number or TCP control code).
- ARP Inspection – Security feature that validates the MAC Address bindings for Address Resolution Protocol packets. Provides protection against ARP traffic with invalid MAC to IP Address bindings, which forms the basis for certain “man-in-the-middle” attacks.
- IP Filter – Filters management access to the web, SNMP or Telnet interface.
- Port Security – Configure secure addresses for individual ports.
- Port Authentication – Use IEEE 802.1X port authentication to control access to specific ports.
- IP Source Guard – Filters untrusted DHCP messages on insecure ports by building and maintaining a DHCP snooping binding table.
- DHCP Snooping – Filter IP traffic on insecure ports for which the source address cannot be identified via DHCP snooping.

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

## AAA AUTHORIZATION AND ACCOUNTING

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

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

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

The switch supports the following AAA features:

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

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

1. Configure RADIUS and TACACS+ server access parameters. See "Configuring Local/Remote Logon Authentication" on page 239.
2. Define RADIUS and TACACS+ server groups to support the accounting and authorization of services.
3. Define a method name for each service to which you want to apply accounting or authorization and specify the RADIUS or TACACS+ server groups to use.
4. Apply the method names to port or line interfaces.

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

## Configuring Local/ Remote Logon Authentication

Use the Security > AAA > System Authentication page to specify local or remote authentication. Local authentication restricts management access based on user names and passwords manually configured on the switch. Remote authentication uses a remote access authentication server based on RADIUS or TACACS+ protocols to verify management access.

### CLI REFERENCES

■"Authentication Sequence" on page 693

### 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. Then specify the corresponding parameters for the remote authentication protocol using the Security > AAA > Server page. Local and remote logon authentication control management access via the console port, web browser, or Telnet.

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

### PARAMETERS

These parameters are displayed in the web interface:

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

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

  - **RADIUS** – User authentication is performed using a RADIUS server only.

  - **TACACS** – User authentication is performed using a TACACS+ server only.

  - [authentication sequence] – User authentication is performed by up to three authentication methods in the indicated sequence.

### WEB INTERFACE

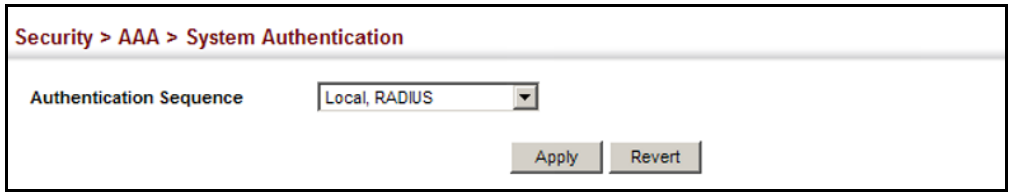
To configure the method(s) of controlling management access:

1. Click Security, AAA, System Authentication.

2. Specify the authentication sequence (i.e., one to three methods).

3. Click Apply.

**Figure 1: Configuring the Authentication Sequence**

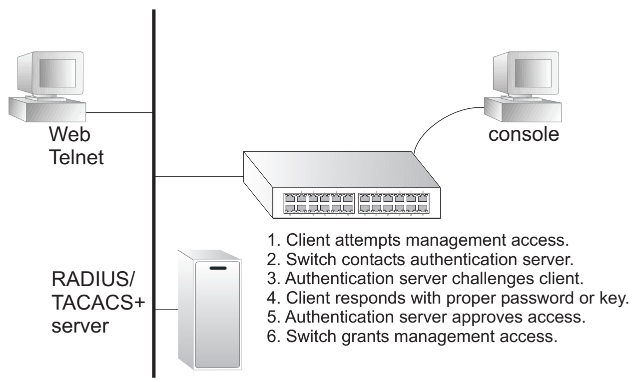



## Configuring Remote Logon Authentication Servers

Use the Security > AAA > Server page to configure the message exchange parameters for RADIUS or TACACS+ remote access authentication servers.

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

**Figure 2: Authentication Server Operation**




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

### CLI REFERENCES

■"RADIUS Client" on page 695
■"TACACS+ Client" on page 700
■"AAA" on page 703

### COMMAND USAGE

■If a remote authentication server is used, you must specify the message exchange parameters for the remote authentication protocol. Both local and remote logon authentication control management access via the console port, web browser, or Telnet.

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

### PARAMETERS

These parameters are displayed in the web interface:

*Configure Server*

■**RADIUS**

- **Global** – Provides globally applicable RADIUS settings.
- **Server Index** – Specifies one of five RADIUS servers that may be configured. The switch attempts authentication using the listed sequence of servers. The process ends when a server either approves or denies access to a user.
- **Server IP Address** – Address of authentication server. (A Server Index entry must be selected to display this item.)
- **Accounting Server UDP Port** – Network (UDP) port on authentication server used for accounting messages. (Range: 1-65535; Default: 1813)
- **Authentication Server UDP Port** – Network (UDP) port on authentication server used for authentication messages. (Range: 1-65535; Default: 1812)
- **Authentication Timeout** – The number of seconds the switch waits for a reply from the RADIUS server before it resends the request. (Range: 1-65535; Default: 5)
- **Authentication Retries** – Number of times the switch tries to authenticate logon access via the authentication server. (Range: 1-30; Default: 2)
- **Set Key** – Mark this box to set or modify the encryption key.
- **Authentication Key** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)
- **Confirm Authentication Key** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the encryption key if these two fields do not match.

■**TACACS+**

- **Global** – Provides globally applicable TACACS+ settings.
- **Server Index** – Specifies the index number of the server to be configured. The switch currently supports only one TACACS+ server.

- **Server IP Address** – Address of the TACACS+ server.
  (A Server Index entry must be selected to display this item.)

- **Authentication Server TCP Port** – Network (TCP) port of TACACS+ server used for authentication messages.
  (Range: 1-65535; Default: 49)

- **Set Key** – Mark this box to set or modify the encryption key.

- **Authentication Key** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)

- **Confirm Authentication Key** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the encryption key if these two fields do not match.

*Configure Group*

- **Server Type** – Select RADIUS or TACACS+ server.

- **Group Name** - Defines a name for the RADIUS or TACACS+ server group. (Range: 1-255 characters)

- **Sequence at Priority** - Specifies the RADIUS server and sequence to use for the group. (Range: 1-5)

  When specifying the priority sequence for a sever, the server index must already be defined (see "Configuring Local/Remote Logon Authentication" on page 239).

### WEB INTERFACE

To configure the parameters for RADIUS or TACACS+ authentication:

1. Click Security, AAA, Server.
2. Select Configure Server from the Step list.
3. Select RADIUS or TACACS+ server type.
4. Select Global to specify the parameters that apply globally to all specified servers, or select a specific Server Index to specify the parameters that apply to a specific server.
5. To set or modify the authentication key, mark the Set Key box, enter the key, and then confirm it
6. Click Apply.

**Figure 3: Configuring Remote Authentication Server** (RADIUS)

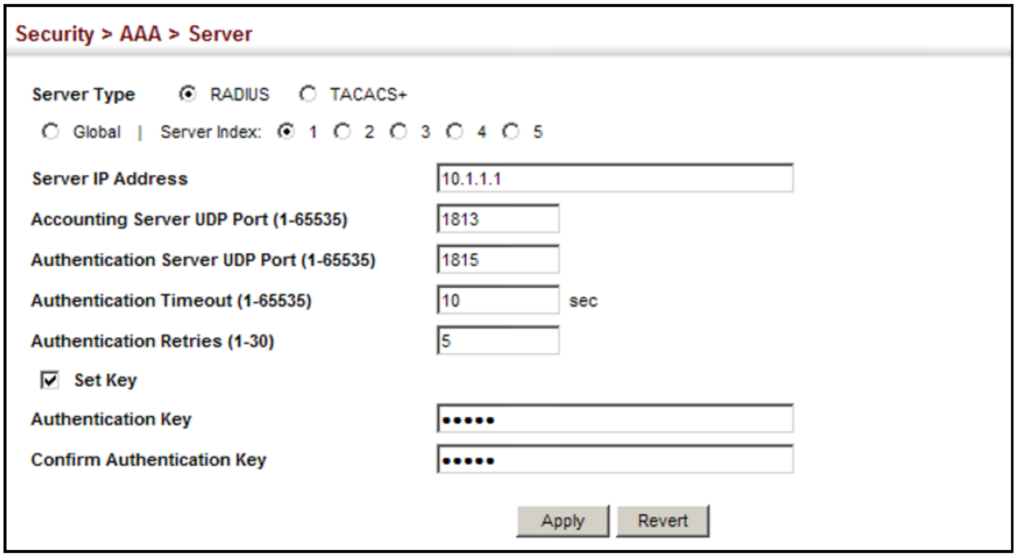
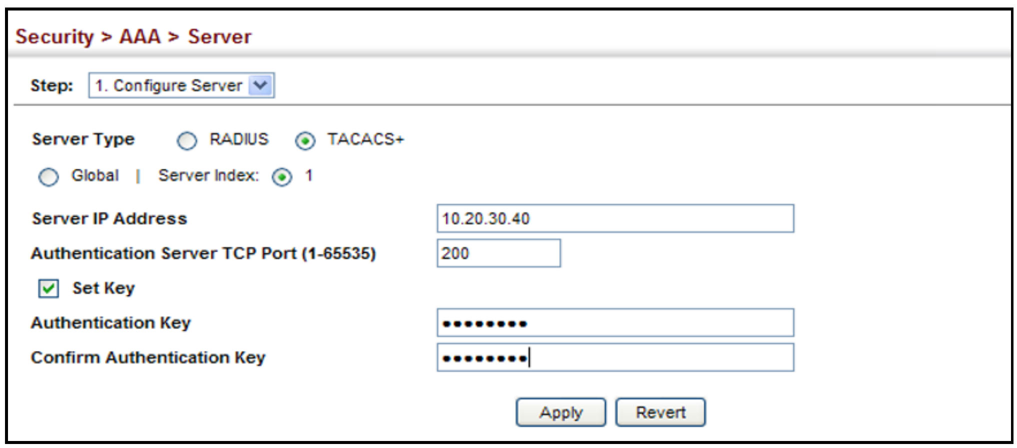


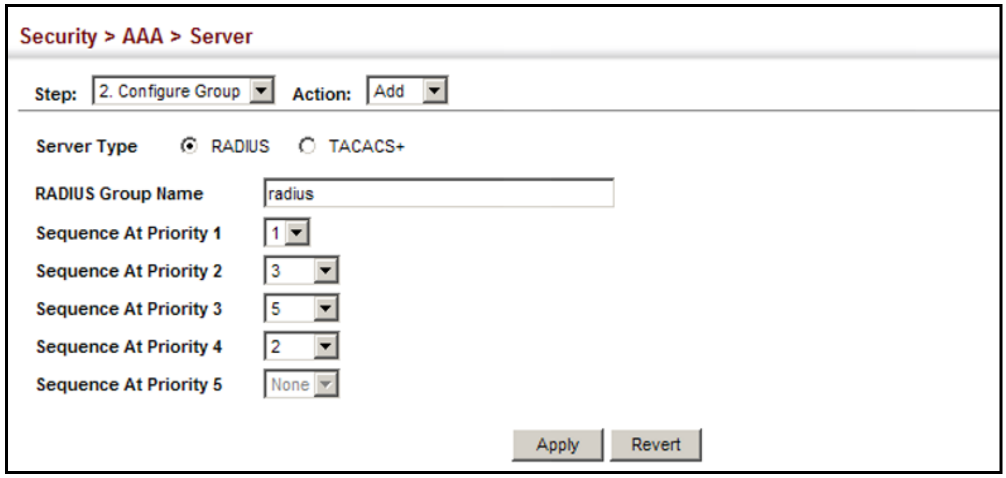

**Figure 4: Configuring Remote Authentication Server** (TACACS+)




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

1. Click Security, AAA, Server.
2. Select Configure Group from the Step list.
3. Select Add from the Action list.
4. Select RADIUS or TACACS+ server type.
5. Enter the group name, followed by the index of the server to use for each priority level.
6. Click Apply.

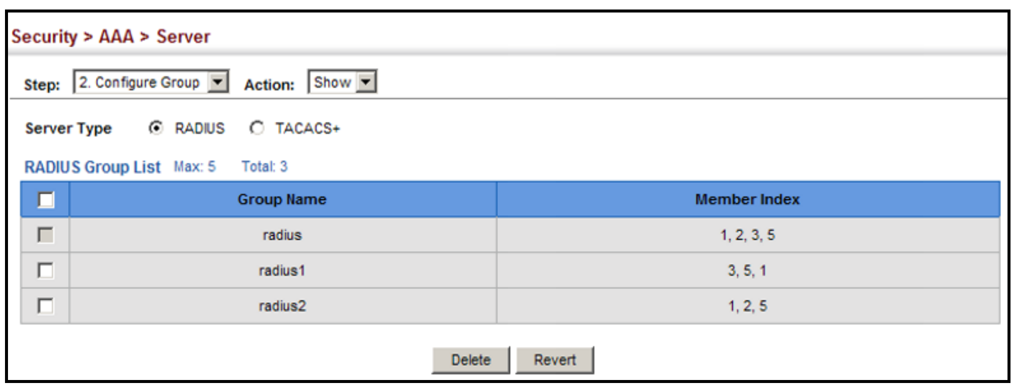
**Figure 5: Configuring AAA Server Groups**




To show the RADIUS or TACACS+ server groups used for accounting and authorization:

1. Click Security, AAA, Server.
2. Select Configure Group from the Step list.
3. Select Show from the Action list.

**Figure 6: Showing AAA Server Groups**




## Configuring AAA Accounting

Use the Security > AAA > Accounting page to enable accounting of requested services for billing or security purposes, and also to display the configured accounting methods, the methods applied to specific interfaces, and basic accounting information recorded for user sessions.

### CLI REFERENCES

■ "AAA" on page 703

### COMMAND USAGE

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

### PARAMETERS

These parameters are displayed in the web interface:

*Configure Global*

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

*Configure Method*

- **Accounting Type** – Specifies the service as:
  - **802.1X** – Accounting for end users.
  - **Exec** – Administrative accounting for local console, Telnet, or SSH connections.
- **Method Name** – Specifies an accounting method for service requests. The "default" methods are used for a requested service if no other methods have been defined. (Range: 1-255 characters)

  Note that the method name is only used to describe the accounting method configured on the specified RADIUS or TACACS+ servers. No information is sent to the servers about the method to use.
- **Accounting Notice** – Records user activity from log-in to log-off point.
- **Server Group Name** - Specifies the accounting server group. (Range: 1-255 characters)

  The group names "radius" and "tacacs+" specifies all configured RADIUS and TACACS+ hosts (see "Configuring Local/Remote Logon Authentication" on page 239). Any other group name refers to a server group configured on the Security > AAA > Server (Configure Group) page.

*Configure Service*

- **Accounting Type** – Specifies the service as 802.1X, Command or Exec as described in the preceding section.
  - **802.1X**
    - **Method Name** – Specifies a user defined accounting method to apply to an interface. This method must be defined in the Configure Method page. (Range: 1-255 characters)
  - **Exec**
    - **Console Method Name** – Specifies a user defined method name to apply to console connections.
    - **Telnet Method Name** – Specifies a user defined method name to apply to Telnet connections.

*Show Information – Summary*

■**Accounting Type** - Displays the accounting service.

■**Method Name** - Displays the user-defined or default accounting method.

■**Server Group Name** - Displays the accounting server group.

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

*Show Information – Statistics*

■**User Name** - Displays a registered user name.

■**Accounting Type** - Displays the accounting service.

■**Interface** - Displays the receive port number through which this user accessed the switch.

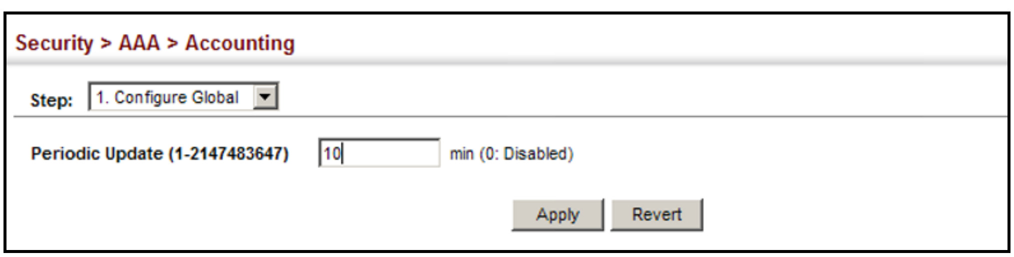
■**Time Elapsed** - Displays the length of time this entry has been active.

### WEB INTERFACE

To configure global settings for AAA accounting:

1. Click Security, AAA, Accounting.
2. Select Configure Global from the Step list.
3. Enter the required update interval.
4. Click Apply.

**Figure 7: Configuring Global Settings for AAA Accounting**




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

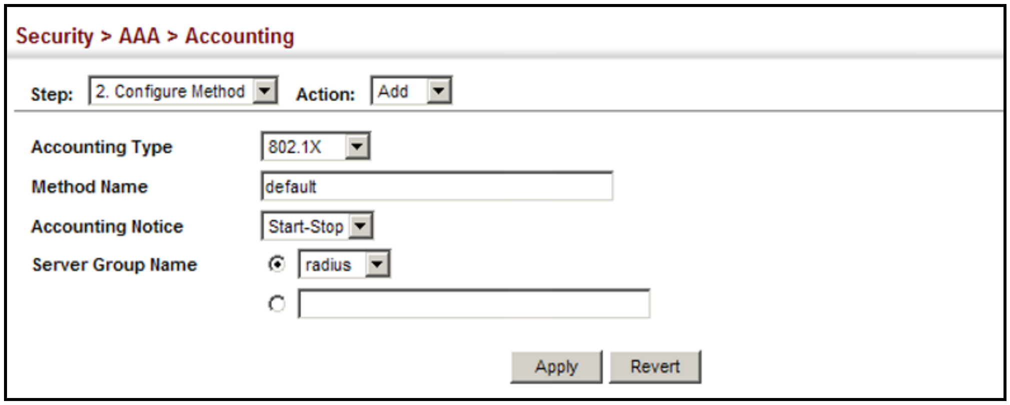
1. Click Security, AAA, Accounting.
2. Select Configure Method from the Step list.
3. Select Add from the Action list.

**4.** Select the accounting type (802.1X, Exec).

**5.** Specify the name of the accounting method and server group name.

**6.** Click Apply.

**Figure 8: Configuring AAA Accounting Methods**



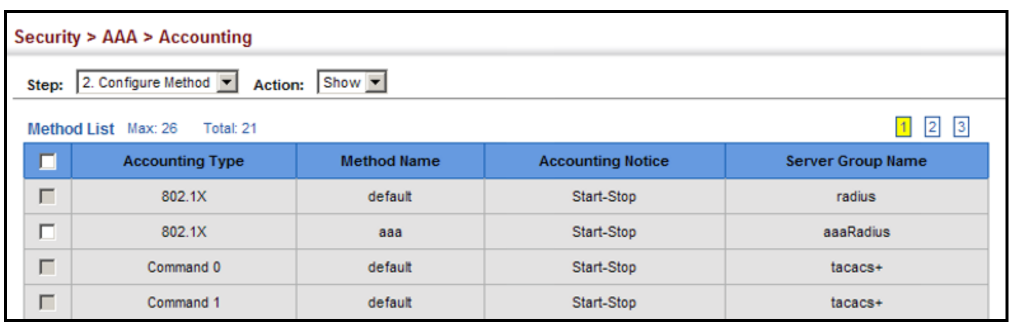

To show the accounting method applied to various service types and the assigned server group:

**1.** Click Security, AAA, Accounting.

**2.** Select Configure Method from the Step list.

**3.** Select Show from the Action list.

**Figure 9: Showing AAA Accounting Methods**




To configure the accounting method applied to specific interfaces, console commands entered at specific privilege levels, and local console, Telnet, or SSH connections:

**1.** Click Security, AAA, Accounting.

**2.** Select Configure Service from the Step list.

**3.** Select the accounting type (802.1X, Exec).

**4.** Enter the required accounting method.

**5.** Click Apply.

**Figure 10: Configuring AAA Accounting Service for 802.1X Service**

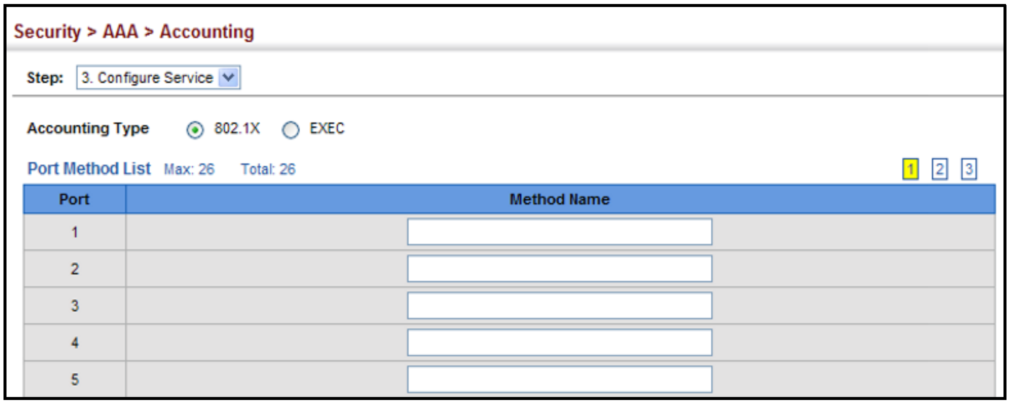
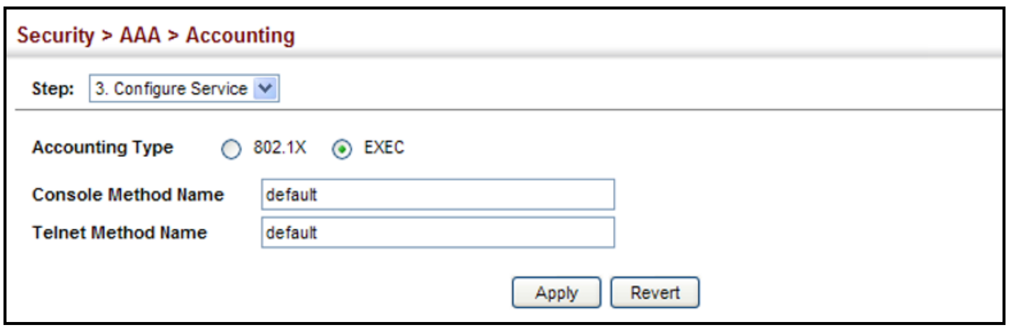



**Figure 11: Configuring AAA Accounting Service for Exec Service**



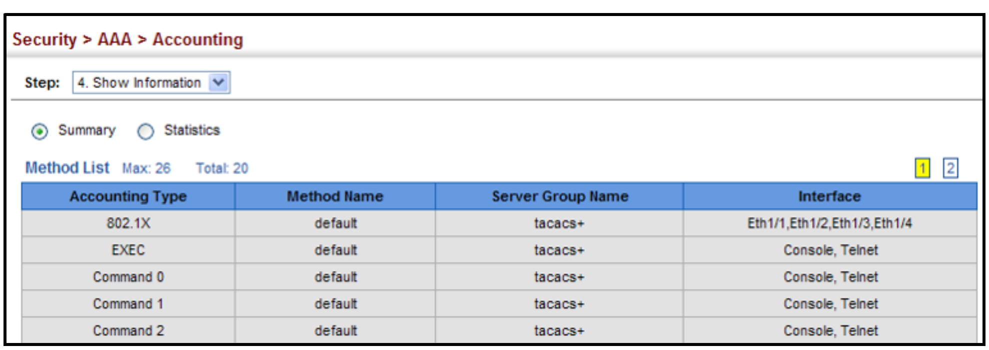

To display a summary of the configured accounting methods and assigned server groups for specified service types:

**1.** Click Security, AAA, Accounting.

**2.** Select Show Information from the Step list.

**3.** Click Summary.

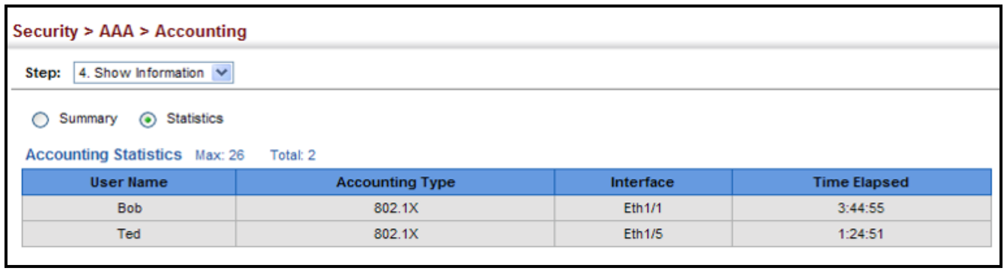
**Figure 12: Displaying a Summary of Applied AAA Accounting Methods**



To display basic accounting information and statistics recorded for user sessions:

1. Click Security, AAA, Accounting.
2. Select Show Information from the Step list.
3. Click Statistics.

**Figure 13: Displaying Statistics for AAA Accounting Sessions**




## Configuring AAA Authorization

Use the Security > AAA > Authorization page to enable authorization of requested services, and also to display the configured authorization methods, and the methods applied to specific interfaces.

### CLI References

■ "AAA" on page 703

### Command Usage

■ This feature performs authorization to determine if a user is allowed to run an Exec shell.

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

### Parameters

These parameters are displayed in the web interface:

*Configure Method*

■ **Authorization Type** – Specifies the service as Exec, indicating administrative authorization for local console, Telnet, or SSH connections.

■ **Method Name** – Specifies an authorization method for service requests. The “default” method is used for a requested service if no other methods have been defined. (Range: 1-255 characters)

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

The group name “tacacs+” specifies all configured TACACS+ hosts (see "Configuring Local/Remote Logon Authentication" on page 239). Any other group name refers to a server group configured on the TACACS+ Group Settings page. Authorization is only supported for TACACS+ servers.

*Configure Service*

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

- **Telnet Method Name** – Specifies a user defined method name to apply to Telnet connections.

*Show Information*

- **Authorization Type** - Displays the authorization service.

- **Method Name** - Displays the user-defined or default accounting method.

- **Server Group Name** - Displays the authorization server group.

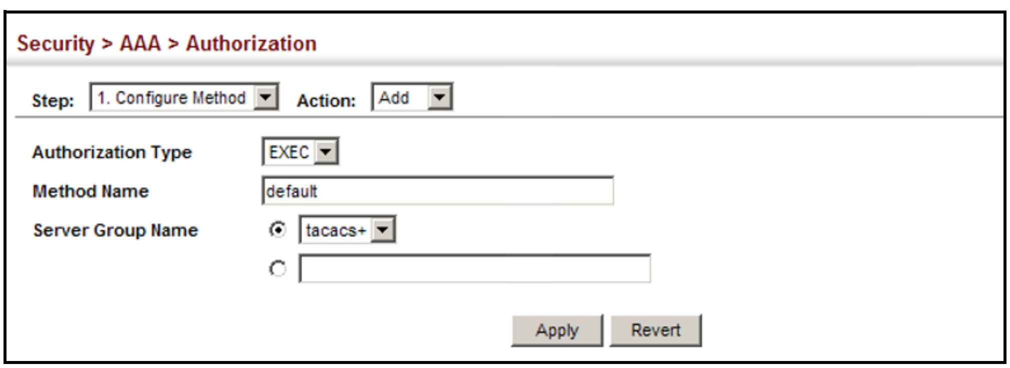
- **Interface** - Displays the console or Telnet interface to which these rules apply. (This field is null if the authorization method and associated server group has not been assigned to an interface.)

### WEB INTERFACE

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

1. Click Security, AAA, Authorization.
2. Select Configure Method from the Step list.
3. Specify the name of the authorization method and server group name.
4. Click Apply.

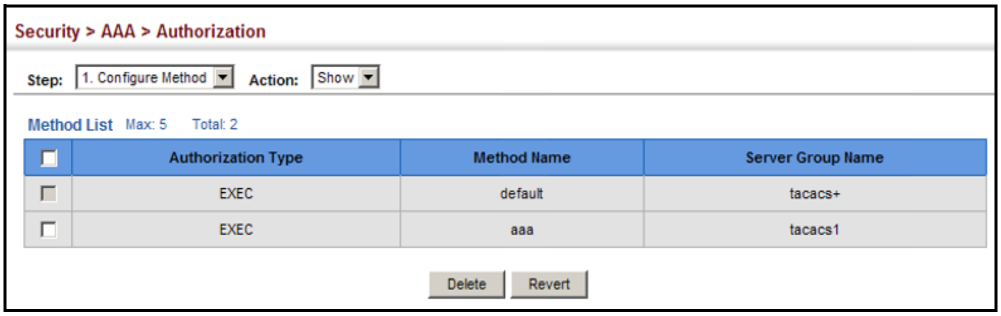
**Figure 14: Configuring AAA Authorization Methods**




To show the authorization method applied to the EXEC service type and the assigned server group:

1. Click Security, AAA, Authorization.
2. Select Configure Method from the Step list.
3. Select Show from the Action list.

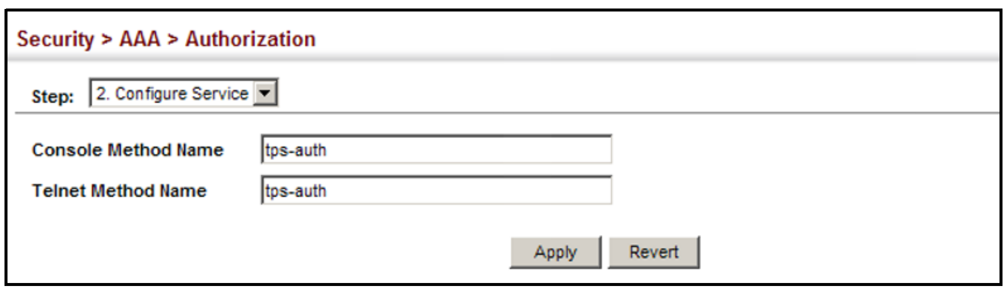
**Figure 15: Showing AAA Authorization Methods**




To configure the authorization method applied to local console, Telnet, or SSH connections:

1. Click Security, AAA, Authorization.
2. Select Configure Service from the Step list.
3. Enter the required authorization method.
4. Click Apply.

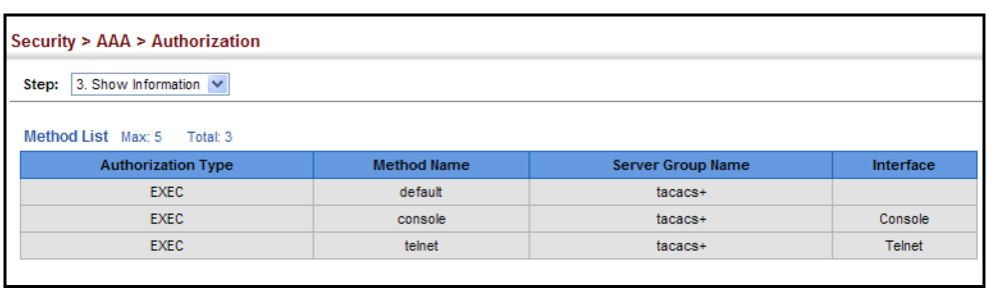
**Figure 16: Configuring AAA Authorization Methods for Exec Service**




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

1. Click Security, AAA, Authorization.
2. Select Show Information from the Step list.

**Figure 17: Displaying the Applied AAA Authorization Method**



# CONFIGURING USER ACCOUNTS

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

### CLI REFERENCES

■ "User Accounts" on page 691

### COMMAND USAGE

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

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

### PARAMETERS

These parameters are displayed in the web interface:

- **User Name** – The name of the user.
  (Maximum length: 8 characters; maximum number of users: 16)

- **Access Level** – Specifies the user level. (Options: 0 - Normal, 15 - Privileged)

  Normal privilege level provides access to a limited number of the commands which display the current status of the switch, as well as several database clear and reset functions. Privileged level provides full access to all commands.

- **Password** – Specifies the user password.
  (Range: 0-8 characters plain text, case sensitive)

- **Confirm Password** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the password if these two fields do not match.

### WEB INTERFACE

To configure user accounts:

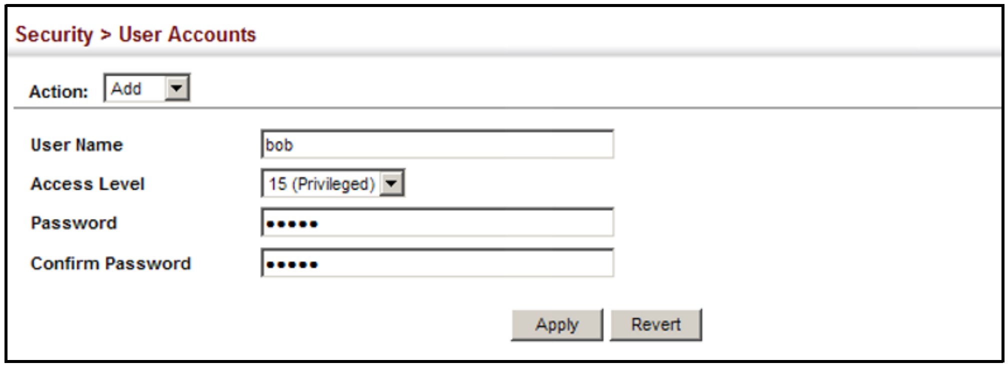
1. Click Security, User Accounts.

2. Select Add from the Action list.

3. Specify a user name, select the user's access level, then enter a password and confirm it.

4. Click Apply.

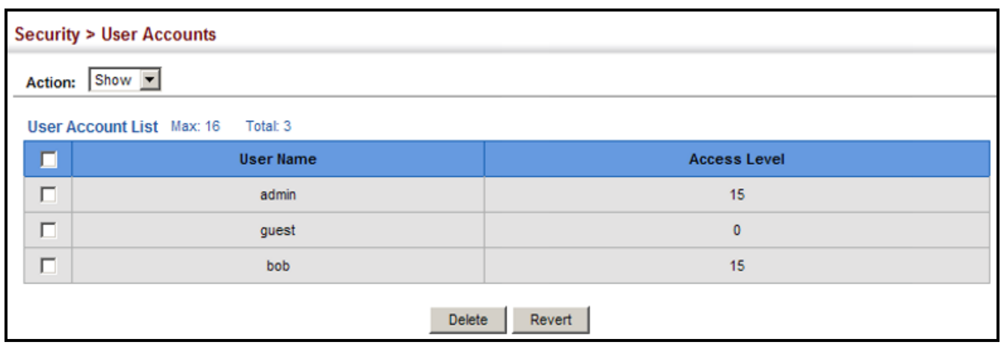
**Figure 18: Configuring User Accounts**




To show user accounts:

1. Click Security, User Accounts.
2. Select Show from the Action list.

**Figure 19: Showing User Accounts**




## WEB AUTHENTICATION

Web authentication allows stations to authenticate and access the network in situations where 802.1X or Network Access authentication are infeasible or impractical. The web authentication feature allows unauthenticated hosts to request and receive a DHCP assigned IP address and perform DNS queries. All other traffic, except for HTTP protocol traffic, is blocked. The switch intercepts HTTP protocol traffic and redirects it to a switch-generated web page that facilitates user name and password authentication via RADIUS. Once authentication is successful, the web browser is forwarded on to the originally requested web page. Successful authentication is valid for all hosts connected to the port.

**NOTE:** RADIUS authentication must be activated and configured properly for the web authentication feature to work properly. (See "Configuring Local/Remote Logon Authentication" on page 239.)

**NOTE:** Web authentication cannot be configured on trunk ports.

## Configuring Global Settings for Web Authentication

Use the Security > Web Authentication (Configure Global) page to edit the global parameters for web authentication.

### CLI REFERENCES

■"Web Authentication" on page 755

### PARAMETERS

These parameters are displayed in the web interface:

■**Web Authentication Status** – Enables web authentication for the switch. (Default: Disabled)

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

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

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

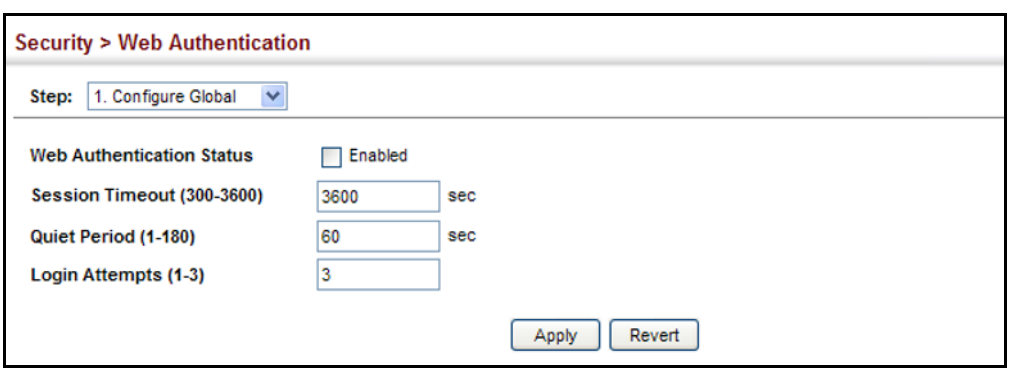
■**Login Attempts** – Configures the amount of times a supplicant may attempt and fail authentication before it must wait the configured quiet period. (Range: 1-3 attempts; Default: 3 attempts)

### WEB INTERFACE

To configure global parameters for web authentication:

1. Click Security, Web Authentication.
2. Select Configure Global from the Step list.
3. Enable web authentication globally on the switch, and adjust any of the protocol parameters as required.
4. Click Apply.

**Figure 20: Configuring Global Settings for Web Authentication**



## Configuring Interface Settings for Web Authentication

Use the Security > Web Authentication (Configure Interface) page to enable web authentication on a port, and display information for any connected hosts.

### CLI REFERENCES

■"Web Authentication" on page 755

### PARAMETERS

These parameters are displayed in the web interface:

■**Port** – Indicates the port being configured.

■**Status** – Configures the web authentication status for the port.

■**Host IP Address** – Indicates the IP address of each connected host.

■**Remaining Session Time** – Indicates the remaining time until the current authorization session for the host expires.

■**Apply** – Enables web authentication if the Status box is checked. Also ends all authenticated web sessions for selected host IP addresses in the Authenticated Host List, and forces the users to re-authenticate.

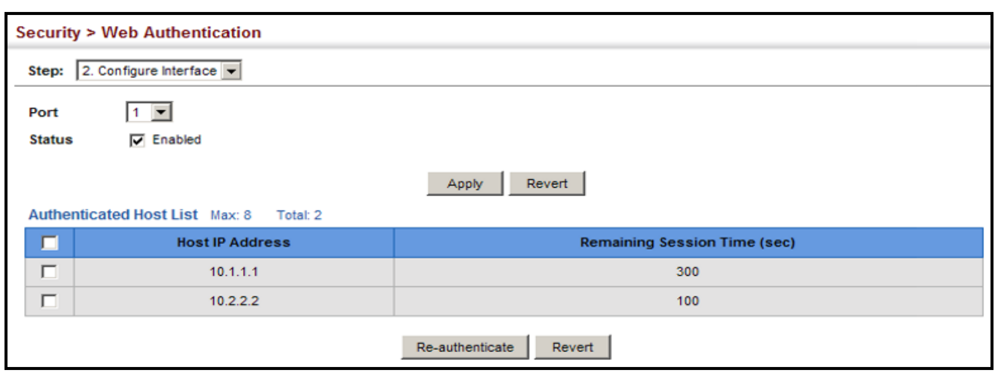
■**Revert** – Restores the previous configuration settings.

### WEB INTERFACE

To enable web authentication for a port:

1. Click Security, Web Authentication.
2. Select Configure Interface from the Step list.
3. Set the status box to enabled for any port that requires web authentication.
4. Mark the check box for any host addresses that need to be re-authenticated.
5. Click Apply.

**Figure 21: Configuring Interface Settings for Web Authentication**



# NETWORK ACCESS (MAC ADDRESS AUTHENTICATION)

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

**NOTE:** RADIUS authentication must be activated and configured properly for the MAC Address authentication feature to work properly. (See "Configuring Remote Logon Authentication Servers" on page 240.)

**NOTE:** MAC authentication cannot be configured on trunk ports.

### CLI REFERENCES

■ "Network Access (MAC Address Authentication)" on page 742

### COMMAND USAGE

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

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

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

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

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

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

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

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

**Table 1: Dynamic QoS Profiles**

| Profile | Attribute Syntax | Example |
|---|---|---|
| DiffServ | **service-policy-in**=*policy-map-name* | service-policy-in=p1 |
| Rate Limit | **rate-limit-input**=*rate* | rate-limit-input=100<br>(in units of Kbps) |
| 802.1p | **switchport-priority-default**=*value* | switchport-priority-default=2 |
| IP ACL | **ip-access-group-in**=*ip-acl-name* | ip-access-group-in=ipv4acl |
| IPv6 ACL | **ipv6-access-group-in**=*ipv6-acl-name* | ipv6-access-group-in=ipv6acl |
| MAC ACL | **mac-access-group-in**=*mac-acl-name* | mac-access-group-in=macAcl |

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

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

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

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

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

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

- When authentication is successful, the dynamic QoS information may not be passed from the RADIUS server due to one of the following conditions (authentication result remains unchanged):

  - The Filter-ID attribute cannot be found to carry the user profile.
  - The Filter-ID attribute is empty.
  - The Filter-ID attribute format for dynamic QoS assignment is unrecognizable (can not recognize the whole Filter-ID attribute).

- Dynamic QoS assignment fails and the authentication result changes from success to failure when the following conditions occur:

  - Illegal characters found in a profile value (for example, a non-digital character in an 802.1p profile value).
  - Failure to configure the received profiles on the authenticated port.

- When the last user logs off on a port with a dynamic QoS assignment, the switch restores the original QoS configuration for the port.

- When a user attempts to log into the network with a returned dynamic QoS profile that is different from users already logged on to the same port, the user is denied access.

- While a port has an assigned dynamic QoS profile, any manual QoS configuration changes only take effect after all users have logged off the port.

## Configuring Global Settings for Network Access

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

### CLI REFERENCES

- "Network Access (MAC Address Authentication)" on page 742

### PARAMETERS

These parameters are displayed in the web interface:

- **Aging Status** – Enables aging for authenticated MAC addresses stored in the secure MAC address table. (Default: Disabled)

  This parameter applies to authenticated MAC addresses configured by the MAC Address Authentication process described in this section, as well as to any secure MAC addresses authenticated by 802.1X, regardless of the 802.1X Operation Mode (Single-Host, Multi-Host, or MAC-Based authentication as described on page 308).

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

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

- **Reauthentication Time** – Sets the time period after which a connected host must be reauthenticated. When the reauthentication time expires for a secure MAC address, it is reauthenticated with the RADIUS server. During the reauthentication process traffic through the port remains unaffected. (Default: 1800 seconds; Range: 120-1000000 seconds)

### WEB INTERFACE

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

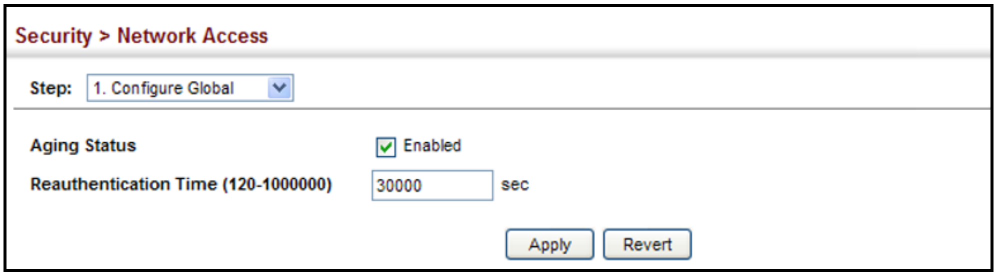
1. Click Security, Network Access.

2. Select Configure Global from the Step list.

3. Enable or disable aging for secure addresses, and modify the reauthentication time as required.

4. Click Apply.

**Figure 22: Configuring Global Settings for Network Access**




## Configuring Network Access for Ports

Use the Security > Network Access (Configure Interface - General) page to configure MAC authentication on switch ports, including enabling address authentication, setting the maximum MAC count, and enabling dynamic VLAN or dynamic QoS assignments.

### CLI REFERENCES

- "Network Access (MAC Address Authentication)" on page 742

### PARAMETERS

These parameters are displayed in the web interface:

- **MAC Authentication**
  - **Status** – Enables MAC authentication on a port. (Default: Disabled)
  - **Intrusion** – Sets the port response to a host MAC authentication failure, to either block access to the port or to pass traffic through. (Options: Block, Pass; Default: Block)
  - **Max MAC Count**[1] – Sets the maximum number of MAC addresses that can be authenticated on a port via MAC authentication; that is, the Network Access process described in this section. (Range: 1-1024; Default: 1024)
- **Network Access Max MAC Count**[1] – Sets the maximum number of MAC addresses that can be authenticated on a port interface via all forms of authentication (including Network Access and IEEE 802.1X). (Range: 1-1024; Default: 1024)
- **Guest VLAN** – Specifies the VLAN to be assigned to the port when 802.1X Authentication fails. (Range: 0-4093, where 0 means disabled; Default: Disabled)

  The VLAN must already be created and active (see "Configuring VLAN Groups" on page 140). Also, when used with 802.1X authentication, intrusion action must be set for “Guest VLAN” (see "Configuring Port Settings for 802.1X" on page 308).
- **Dynamic VLAN** – Enables dynamic VLAN assignment for an authenticated port. When enabled, any VLAN identifiers returned by the RADIUS server are applied to the port, providing the VLANs have already been created on the switch. (GVRP is not used to create the VLANs.) (Default: Enabled)

1. The maximum number of MAC addresses per port is 1024, and the maximum number of secure MAC addresses supported for the switch system is 1024. When the limit is reached, all new MAC addresses are treated as authentication failures.

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

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

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

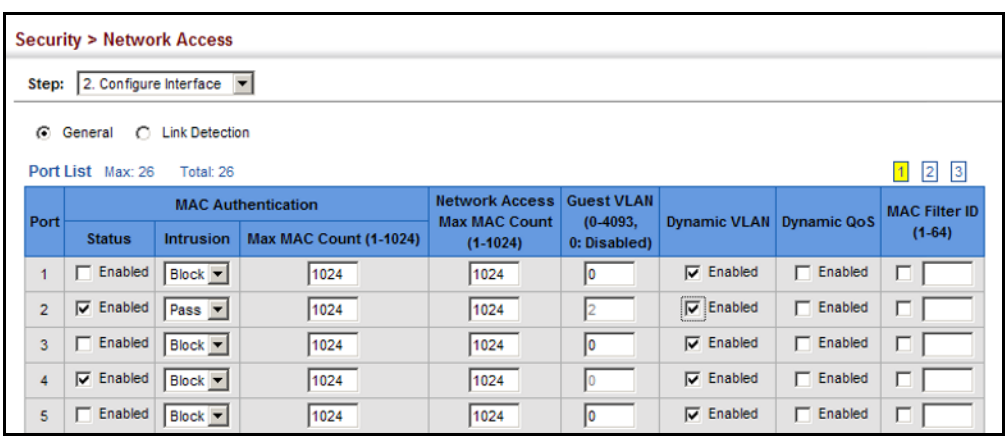
- **Dynamic QoS** – Enables dynamic QoS assignment for an authenticated port. (Default: Disabled)
- **MAC Filter ID** – Allows a MAC Filter to be assigned to the port. MAC addresses or MAC address ranges present in a selected MAC Filter are exempt from authentication on the specified port (as described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

### WEB INTERFACE

To configure MAC authentication on switch ports:

1. Click Security, Network Access.
2. Select Configure Interface from the Step list.
3. Click the General button.
4. Make any configuration changes required to enable address authentication on a port, set the maximum number of secure addresses supported, the guest VLAN to use when MAC Authentication or 802.1X Authentication fails, and the dynamic VLAN and QoS assignments.
5. Click Apply.

**Figure 23: Configuring Interface Settings for Network Access**



## Configuring Port Link Detection

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

### CLI References

■ "Network Access (MAC Address Authentication)" on page 742

### Parameters

These parameters are displayed in the web interface:

■ **Link Detection Status** – Configures whether Link Detection is enabled or disabled for a port.

■ **Condition** – The link event type which will trigger the port action.

- ◆ **Link up** – Only link up events will trigger the port action.
- ◆ **Link down** – Only link down events will trigger the port action.
- ◆ **Link up and down** – All link up and link down events will trigger the port action.

■ **Action** – The switch can respond in three ways to a link up or down trigger event.

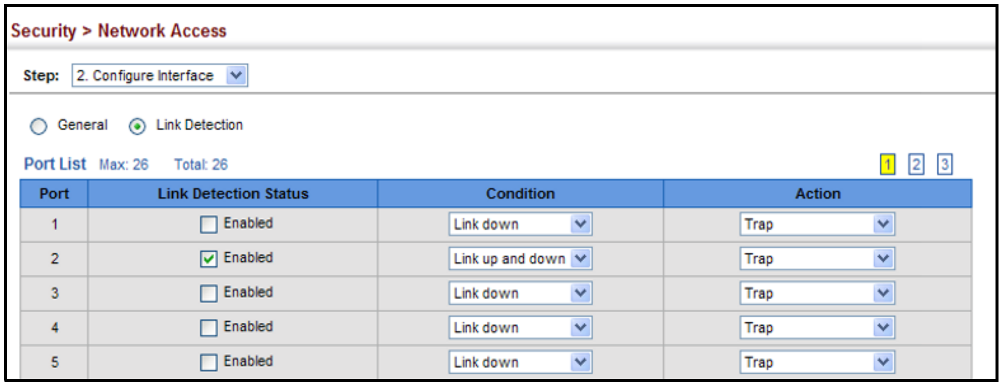
- ◆ **Trap** – An SNMP trap is sent.
- ◆ **Trap and shutdown** – An SNMP trap is sent and the port is shut down.
- ◆ **Shutdown** – The port is shut down.

### Web Interface

To configure link detection on switch ports:

1. Click Security, Network Access.
2. Select Configure Interface from the Step list.
3. Click the Link Detection button.
4. Modify the link detection status, trigger condition, and the response for any port.
5. Click Apply.

**Figure 24: Configuring Link Detection for Network Access**




## Configuring a MAC Address Filter

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

### CLI REFERENCES

■"Network Access (MAC Address Authentication)" on page 742

### COMMAND USAGE

■Specified MAC addresses are exempt from authentication.

■Up to 65 filter tables can be defined.

■There is no limitation on the number of entries used in a filter table.

### PARAMETERS

These parameters are displayed in the web interface:

■**Filter ID** – Adds a filter rule for the specified filter.

■**MAC Address** – The filter rule will check ingress packets against the entered MAC address or range of MAC addresses (as defined by the MAC Address Mask).

■**MAC Address Mask** – The filter rule will check for the range of MAC addresses defined by the MAC bit mask. If you omit the mask, the system will assign the default mask of an exact match. (Range: 000000000000 - FFFFFFFFFFFF; Default: FFFFFFFFFFFF)

### WEB INTERFACE

To add a MAC address filter for MAC authentication:

**1.** Click Security, Network Access.

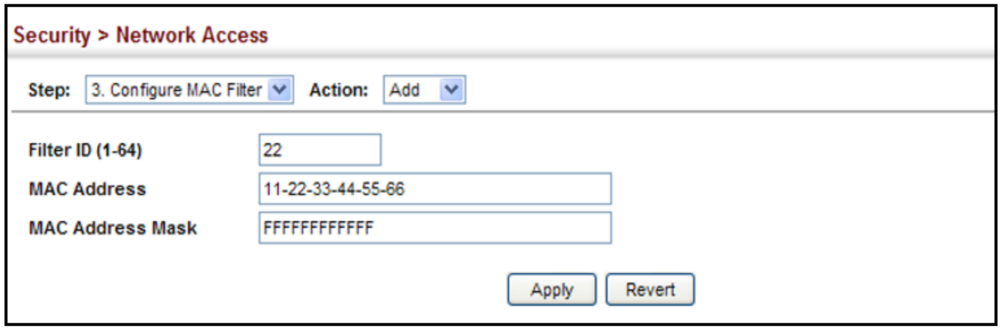
**2.** Select Configure MAC Filter from the Step list.

**3.** Select Add from the Action list.

4. Enter a filter ID, MAC address, and optional mask.

5. Click Apply.

**Figure 25: Configuring a MAC Address Filter for Network Access**



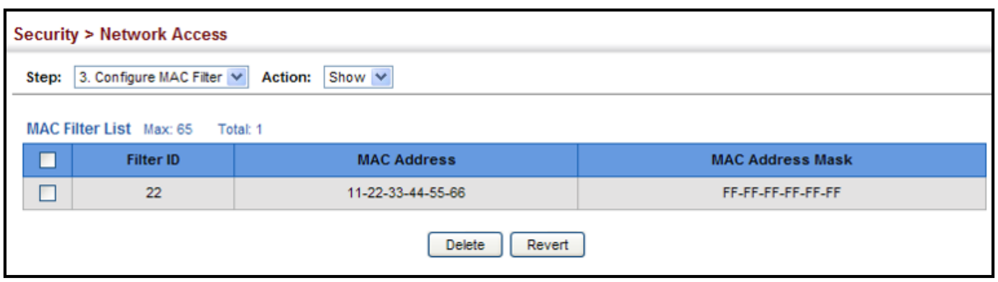

To show the MAC address filter table for MAC authentication:

1. Click Security, Network Access.

2. Select Configure MAC Filter from the Step list.

3. Select Show from the Action list.

**Figure 26: Showing the MAC Address Filter Table for Network Access**




## Displaying Secure MAC Address Information

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

### CLI REFERENCES

■ "Network Access (MAC Address Authentication)" on page 742

### PARAMETERS

These parameters are displayed in the web interface:

■ **Query By** – Specifies parameters to use in the MAC address query.

- ◆ **Sort Key** – Sorts the information displayed based on MAC address, port interface, or attribute.

- **MAC Address** – Specifies a specific MAC address.
- **Interface** – Specifies a port interface.
- **Attribute** – Displays static or dynamic addresses.

■**Authenticated MAC Address List**

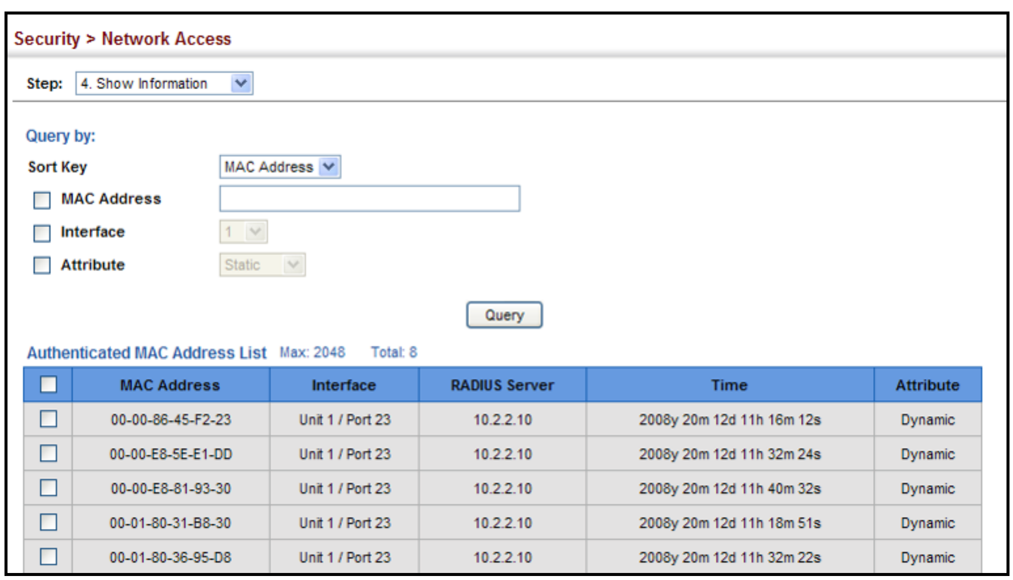
- **MAC Address** – The authenticated MAC address.
- **Interface** – The port interface associated with a secure MAC address.
- **RADIUS Server** – The IP address of the RADIUS server that authenticated the MAC address.
- **Time** – The time when the MAC address was last authenticated.
- **Attribute**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

### WEB INTERFACE

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

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

**Figure 27: Showing Addresses Authenticated for Network Access**



# CONFIGURING HTTPS

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

## Configuring Global Settings for HTTPS

Use the Security > HTTPS (Configure Global) page to enable or disable HTTPS and specify the UDP port used for this service.

### CLI REFERENCES

- "Web Server" on page 711

### COMMAND USAGE

- Both the HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure both services to use the same UDP port. (HTTP can only be configured through the CLI using the ip http server command described on page 712.)

- If you enable HTTPS, you must indicate this in the URL that you specify in your browser: https://*device*[:*port_number*]

- When you start HTTPS, the connection is established in this way:
  - The client authenticates the server using the server's digital certificate.
  - The client and server negotiate a set of security protocols to use for the connection.
  - The client and server generate session keys for encrypting and decrypting data.

- The client and server establish a secure encrypted connection.

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

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

**Table 2: HTTPS System Support**

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

- To specify a secure-site certificate, see "Replacing the Default Secure-site Certificate" on page 266.

### PARAMETERS

These parameters are displayed in the web interface:

- **HTTPS Status** – Allows you to enable/disable the HTTPS server feature on the switch. (Default: Enabled)

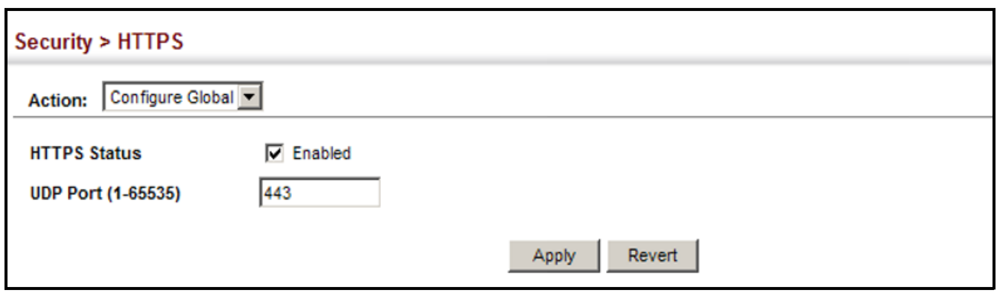
- **HTTPS Port** – Specifies the UDP port number used for HTTPS connection to the switch's web interface. (Default: Port 443)

### WEB INTERFACE

To configure HTTPS:

1. Click Security, HTTPS.
2. Select Configure Global from the Step list.
3. Enable HTTPS and specify the port number if required.
4. Click Apply.

**Figure 28: Configuring HTTPS**




## Replacing the Default Secure-site Certificate

Use the Security > HTTPS (Copy Certificate) page to replace the default secure-site certificate.

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

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

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

**Note:** The switch must be reset for the new certificate to be activated. To reset the switch, see "Resetting the System" on page 103 or type “reload” at the command prompt: ES-3026#reload

### CLI References

■ "Web Server" on page 711

### Parameters

These parameters are displayed in the web interface:

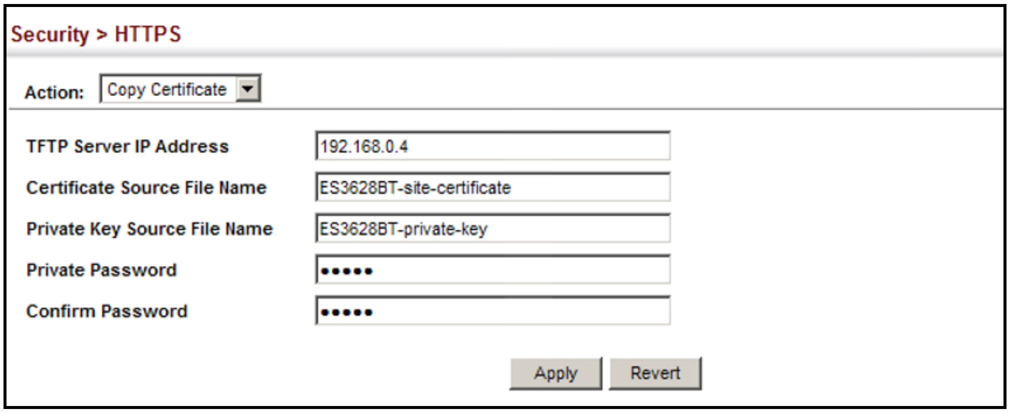
- **TFTP Server IP Address** – IP address of TFTP server which contains the certificate file.
- **Certificate Source File Name** – Name of certificate file stored on the TFTP server.
- **Private Key Source File Name** – Name of private key file stored on the TFTP server.
- **Private Password** – Password stored in the private key file. This password is used to verify authorization for certificate use, and is verified when downloading the certificate to the switch.
- **Confirm Password** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not download the certificate if these two fields do not match.

### Web Interface

To replace the default secure-site certificate:

1. Click Security, HTTPS.
2. Select Copy Certificate from the Step list.
3. Fill in the TFTP server, certificate and private key file name, and private password.
4. Click Apply.

**Figure 29: Downloading the Secure-Site Certificate**




## CONFIGURING THE SECURE SHELL

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

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

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

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

### COMMAND USAGE

The SSH server on this switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified on the System Authentication page (page 239). 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
   595664104869574278881462065194174677298486546861571773939016477935594230
   357741309802273708779454524083971752646358058176716709574804776117

3. *Import Client's Public Key to the Switch* – See "Importing User Public Keys" on page 273, or use the copy tftp public-key command (page 625) 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 252.) 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
   1341081685609893921040944920155425347631641921872958921143173880055536161
   631051775940838686311092912322268285192543746031009371877211996963178136
   627741416898513204911720483033925432410163799759237144901193800609025394
   840848271781943722884025331159521348610229029789827213532671316294325328
   18915045306393916643 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. Authentication – One of the following authentication methods is employed:

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

   a. **The client sends its password to the server.**
   b. The switch compares the client's password to those stored in memory.
   c. If a match is found, the connection is allowed.

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

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

*Authenticating SSH v1.5 Clients*

**a.The client sends its RSA public key to the switch.**

**b.**The switch compares the client's public key to those stored in memory.

**c.**If a match is found, the switch uses its secret key to generate a random 256-bit string as a challenge, encrypts this string with the user’s public key, and sends it to the client.

**d.**The client uses its private key to decrypt the challenge string, computes the MD5 checksum, and sends the checksum back to the switch.

**e.**The switch compares the checksum sent from the client against that computed for the original string it sent. If the two checksums match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

*Authenticating SSH v2 Clients*

**a.The client first queries the switch to determine if DSA public key authentication using a preferred algorithm is acceptable.**

**b.**If the specified algorithm is supported by the switch, it notifies the client to proceed with the authentication process. Otherwise, it rejects the request.

**c.**The client sends a signature generated using the private key to the switch.

**d.**When the server receives this message, it checks whether the supplied key is acceptable for authentication, and if so, it then checks whether the signature is correct. If both checks succeed, the client is authenticated.

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

**NOTE:** The SSH server can be accessed using any configured IPv4 or IPv6 interface address on the switch.

## Configuring the SSH Server

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

**NOTE:** A host key pair must be configured on the switch before you can enable the SSH server. See "Generating the Host Key Pair" on page 272.

### CLI REFERENCES

- "Secure Shell" on page 716

### PARAMETERS

These parameters are displayed in the web interface:

- **SSH Server Status** – Allows you to enable/disable the SSH server on the switch. (Default: Disabled)

- **Version** – The Secure Shell version number. Version 2.0 is displayed, but the switch supports management access via either SSH Version 1.5 or 2.0 clients.

- **Authentication Timeout** – Specifies the time interval in seconds that the SSH server waits for a response from a client during an authentication attempt. (Range: 1-120 seconds; Default: 120 seconds)

- **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)

- **Server-Key Size** – Specifies the SSH server key size. (Range: 512-896 bits; Default:768)

  - The server key is a private key that is never shared outside the switch.

  - The host key is shared with the SSH client, and is fixed at 1024 bits.

### WEB INTERFACE

To configure the SSH server:

1. Click Security, SSH.

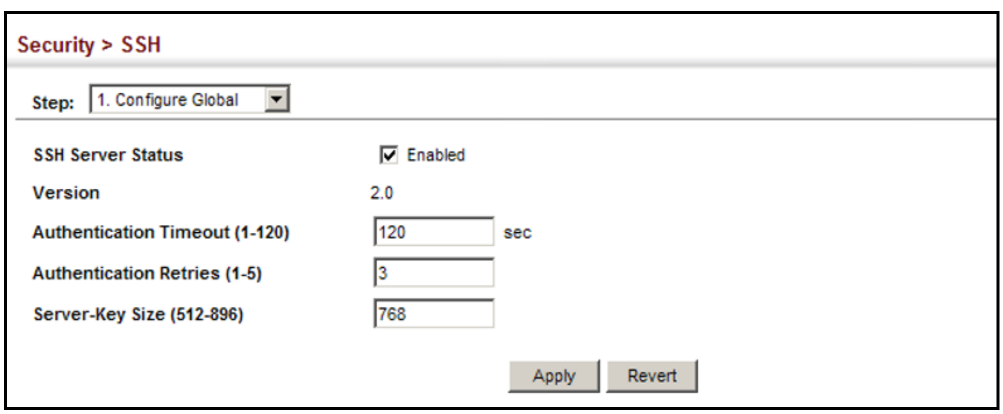
2. Select Configure Global from the Step list.

3. Enable the SSH server.

4. Adjust the authentication parameters as required.

5. Click Apply.

**Figure 30: Configuring the SSH Server**



## Generating the Host Key Pair

Use the Security > SSH (Configure Host Key - Generate) page to generate a host public/private key pair used to provide secure communications between an SSH client and the switch. After generating this key pair, you must provide the host public key to SSH clients and import the client's public key to the switch as described in the section "Importing User Public Keys" on page 273.

**NOTE:** A host key pair must be configured on the switch before you can enable the SSH server. See "Configuring the SSH Server" on page 270.

### CLI REFERENCES

- "Secure Shell" on page 716

### PARAMETERS

These parameters are displayed in the web interface:

- **Host-Key Type** – The key type used to generate the host key pair (i.e., public and private keys). (Range: RSA (Version 1), DSA (Version 2), Both; Default: Both)

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

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

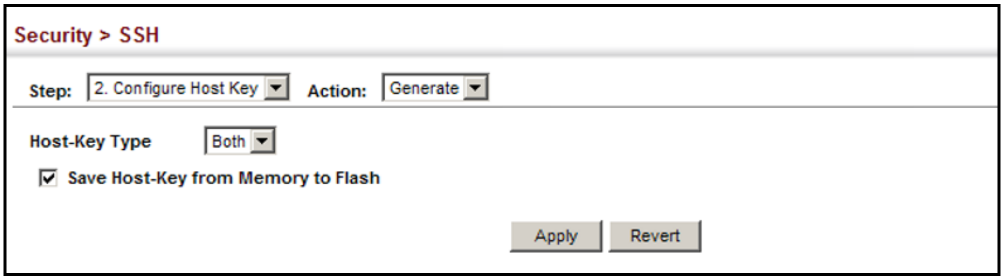
- **Save Host-Key from Memory to Flash** – Saves the host key from RAM (i.e., volatile memory) to flash memory. Otherwise, the host key pair is stored to RAM by default. Note that you must select this item prior to generating the host-key pair. (Default: Disabled)

### WEB INTERFACE

To generate the SSH host key pair:

1. Click Security, SSH.
2. Select Configure Host Key from the Step list.
3. Select Generate from the Action list.
4. Select the host-key type from the drop-down box.
5. Select the option to save the host key from memory to flash if required.
6. Click Apply.

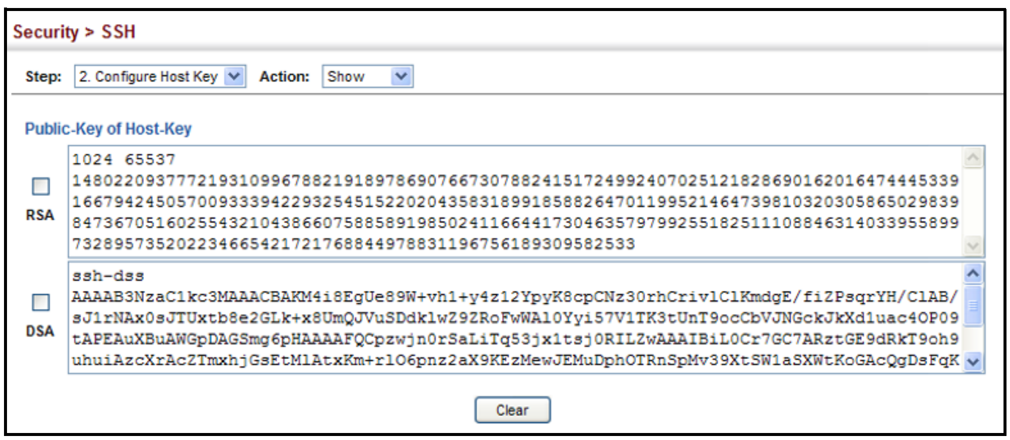
**Figure 31: Generating the SSH Host Key Pair**




To display or clear the SSH host key pair:

1. Click Security, SSH.
2. Select Configure Host Key from the Step list.
3. Select Show from the Action list.
4. Select the host-key type to clear.
5. Click Show.

**Figure 32: Showing the SSH Host Key Pair**




## Importing User Public Keys

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

### CLI REFERENCES

■ "Secure Shell" on page 716

### PARAMETERS

These parameters are displayed in the web interface:

- **User Name** – This drop-down box selects the user who's public key you wish to manage. Note that you must first create users on the User Accounts page (see "Configuring User Accounts" on page 252).

- **User Key Type** – The type of public key to upload.

  - RSA: The switch accepts a RSA version 1 encrypted public key.

  - DSA: The switch accepts a DSA version 2 encrypted public key.

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

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

- **TFTP Server IP Address** – The IP address of the TFTP server that contains the public key file you wish to import.

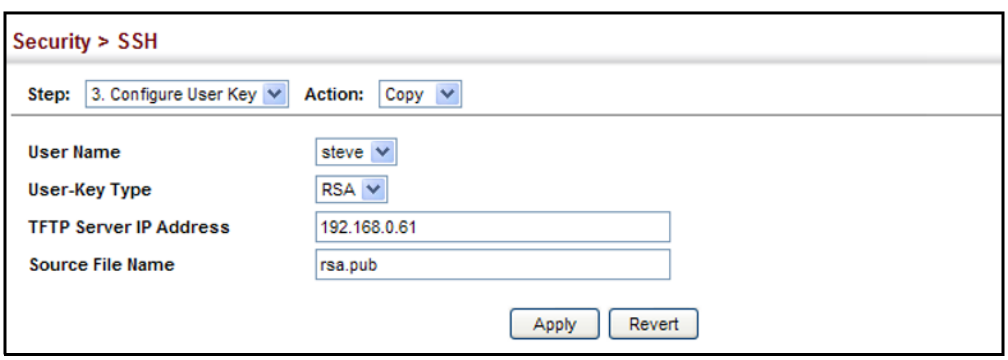
- **Source File Name** – The public key file to upload.

### WEB INTERFACE

To copy the SSH user's public key:

1. Click Security, SSH.
2. Select Configure User Key from the Step list.
3. Select Copy from the Action list.
4. Select the user name and the public-key type from the respective drop-down boxes, input the TFTP server IP address and the public key source file name.
5. Click Apply.

**Figure 33: Copying the SSH User's Public Key**



To display or clear the SSH user's public key:

1. Click Security, SSH.
2. Select Configure User Key from the Step list.
3. Select Show from the Action list.
4. Select a user from the User Name list.
5. Select the host-key type to clear.
6. Click Clear.

**Figure 34: Showing the SSH User's Public Key**


## ACCESS CONTROL LISTS

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

*Configuring Access Control Lists –*

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

### COMMAND USAGE

The following restrictions apply to ACLs:

- The maximum number of ACLs is 32.

- The maximum number of rules per ACL is 96.
- The maximum number of rules that can be bound to the ports is 96 for each of the following list types: MAC ACLs, IP ACLs (including Standard and Extended ACLs), IPv6 Standard ACLs, and IPv6 Extended ACLs. For the EL326, all ports share this quota.
- The order in which active ACLs are checked is as follows:

1. User-defined rules in IP and MAC ACLs for ingress ports are checked in parallel.
2. Rules within an ACL are checked in the configured order, from top to bottom.
3. If the result of checking an IP ACL is to permit a packet, but the result of a MAC ACL on the same packet is to deny it, the packet will be denied (because the decision to deny a packet has a higher priority for security reasons). A packet will also be denied if the IP ACL denies it and the MAC ACL accepts it.

## Setting A Time Range

Use the Security > ACL (Configure Time Range) page to sets a time range during which ACL functions are applied.

**CLI REFERENCES**

- "Time Range" on page 654

**PARAMETERS**

These parameters are displayed in the web interface:

*Add*

- **Time-Range Name** – Name of a time range. (Range: 1-30 characters)

*Add Rule*

- **Time-Range** – Name of a time range.
- **Mode**
  - **Absolute** – Specifies a specific time or time range.
    - **Start/End** – Specifies the hours, minutes, month, day, and year at which to start or end.
  - **Periodic** – Specifies a periodic interval.
    - **Start/To** – Specifies the days of the week, hours, and minutes at which to start or end.

**WEB INTERFACE**

To configure a time range:

1. Click Security, ACL.

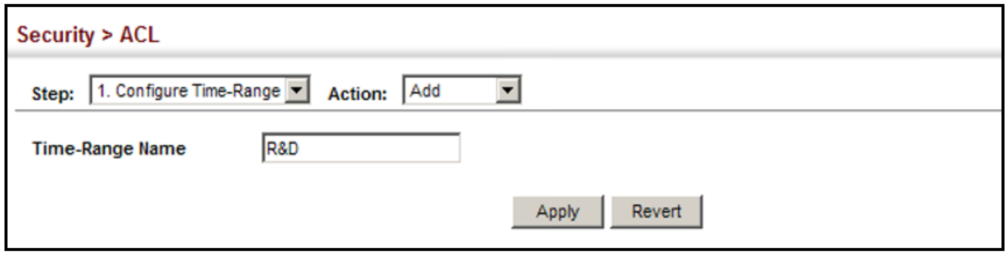
2. Select Configure Time Range from the Step list.

3. Select Add from the Action list.

4. Enter the name of a time range.

5. Click Apply.

**Figure 35: Setting the Name of a Time Range**



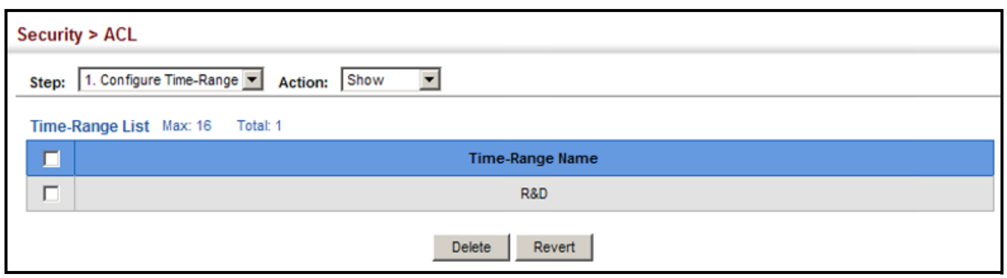

To show a list of time ranges:

1. Click Security, ACL.

2. Select Configure Time Range from the Step list.

3. Select Show from the Action list.

**Figure 36: Showing a List of Time Ranges**




To configure a rule for a time range:

1. Click Security, ACL.

2. Select Configure Time Range from the Step list.

3. Select Add Rule from the Action list.

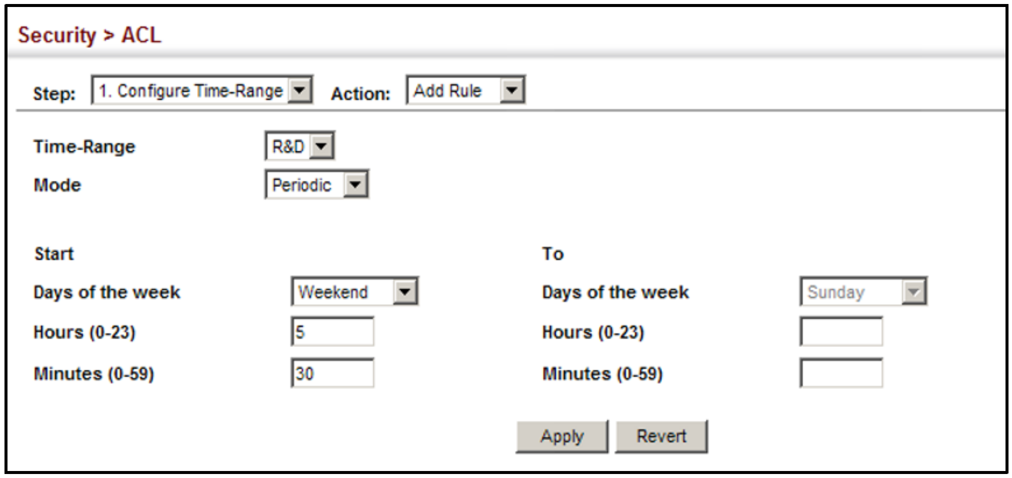
4. Select the name of time range from the drop-down list.

5. Select a mode option of Absolute or Periodic.

6. Fill in the required parameters for the selected mode.

7. Click Apply.

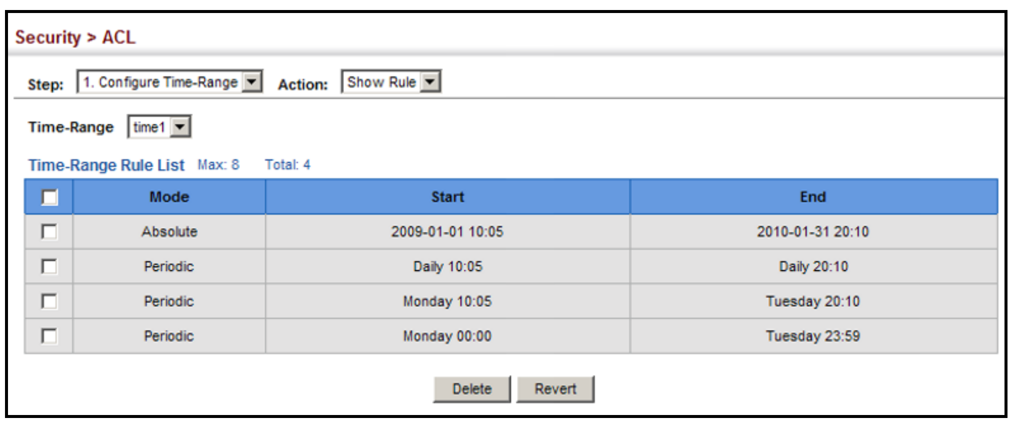
**Figure 37: Add a Rule to a Time Range**




To show the rules configured for a time range:

1. Click Security, ACL.
2. Select Configure Time Range from the Step list.
3. Select Show Rule from the Action list.

**Figure 38: Showing the Rules Configured for a Time Range**



## Showing TCAM Utilization

Use the Security > ACL (Configure ACL - Show TCAM) page to show utilization parameters for TCAM (Ternary Content Addressable Memory), including the number policy control entries in use, the number of free entries, and the overall percentage of TCAM in use.

### CLI REFERENCES

■"show access-list tcam-utilization" on page 616

### COMMAND USAGE

Policy control entries (PCEs) are used by various system functions which rely on rule-based searches, including Access Control Lists (ACLs), IP Source Guard filter rules, Quality of Service (QoS) processes, or traps.

For example, when binding an ACL to a port, each rule in an ACL will use two PCEs; and when setting an IP Source Guard filter rule for a port, the system will also use two PCEs.

### PARAMETERS

These parameters are displayed in the web interface:

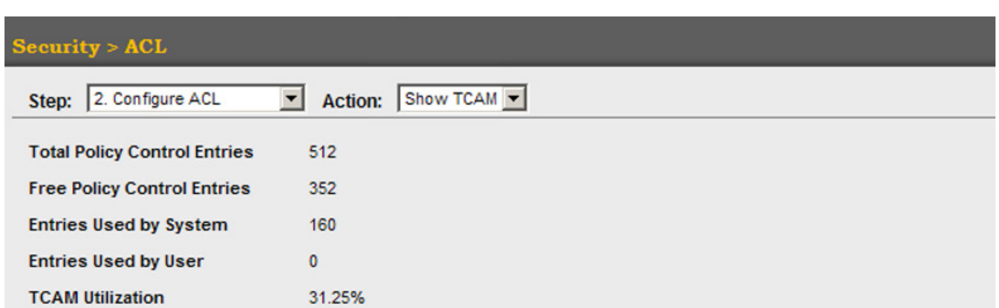
- **Total Policy Control Entries** – The number policy control entries in use.
- **Free Policy Control Entries** – The number of policy control entries available for use.
- **Entries Used by System** – The number of policy control entries used by the operating system.
- **Entries Used by User** – The number of policy control entries used by configuration settings, such as access control lists.
- **TCAM Utilization** – The overall percentage of TCAM in use.

### WEB INTERFACE

To show information on TCAM utilization in the web interface:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Show TCM from the Action list.

**Figure 39: Showing TCAM Utilization**



## Setting the ACL Name and Type

Use the Security > ACL (Configure ACL - Add) page to create an ACL.

**CLI REFERENCES**


- "access-list ip" on page 784
- "show ip access-list" on page 789


**PARAMETERS**

These parameters are displayed in the web interface:

- **ACL Name** – Name of the ACL. (Maximum length: 15 characters)

- **Type** – The following filter modes are supported:

  - **IP Standard**: IPv4 ACL mode filters packets based on the source IPv4 address.

  - **IP Extended**: IPv4 ACL mode filters packets based on the source or destination IPv4 address, as well as the protocol type and protocol port number. If the “TCP” protocol is specified, then you can also filter packets based on the TCP control code.

  - **IPv6 Standard**: IPv6 ACL mode filters packets based on the source IPv6 address.

  - **IPv6 Extended**: IPv6 ACL mode filters packets based on the source or destination IP address, as well as the type of the next header and the flow label (i.e., a request for special handling by IPv6 routers).

  - **MAC** – MAC ACL mode filters packets based on the source or destination MAC address and the Ethernet frame type (RFC 1060).

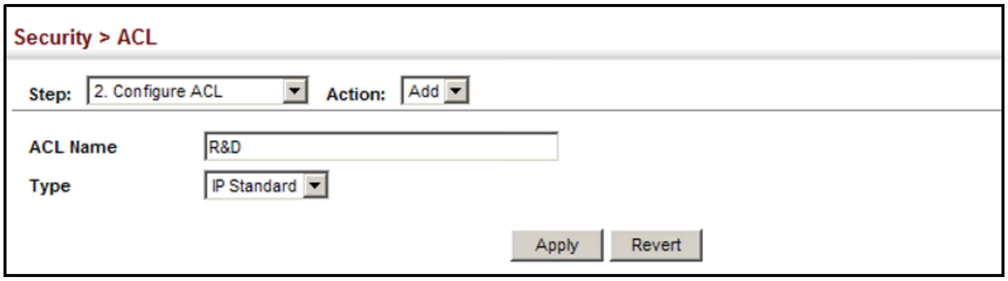
  - **ARP** – ARP ACL specifies static IP-to-MAC address bindings used for ARP inspection (see "ARP Inspection" on page 294).

**WEB INTERFACE**

To configure the name and type of an ACL:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Add from the Action list.
4. Fill in the ACL Name field, and select the ACL type.
5. Click Apply.

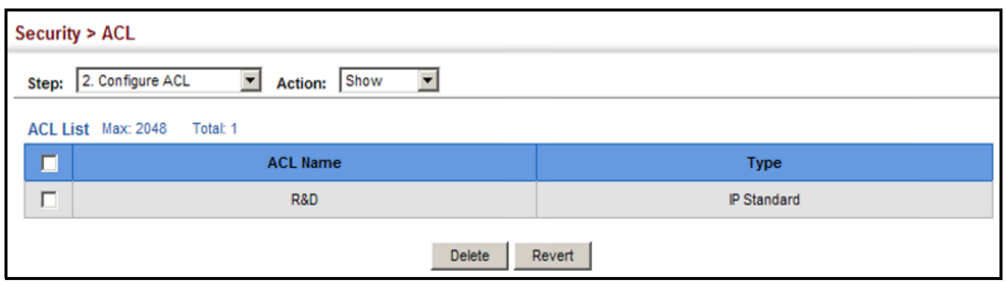
**Figure 40: Creating an ACL**




To show a list of ACLs:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Show from the Action list.

**Figure 41: Showing a List of ACLs**




## Configuring a Standard IPv4 ACL

Use the Security > ACL (Configure ACL - Add Rule - IP Standard) page to configure a Standard IPv4 ACL.

### CLI REFERENCES

- "permit, deny (Standard IP ACL)" on page 785
- "show ip access-list" on page 789
- "Time Range" on page 654

### PARAMETERS

These parameters are displayed in the web interface:

- **Type** – Selects the type of ACLs to show in the Name list.
- **Name** – Shows the names of ACLs matching the selected type.
- **Action** – An ACL can contain any combination of permit or deny rules.
- **Address Type** – Specifies the source IP address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and Subnet Mask fields. (Options: Any, Host, IP; Default: Any)

- **Source IP Address** – Source IP address.

- **Source 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.

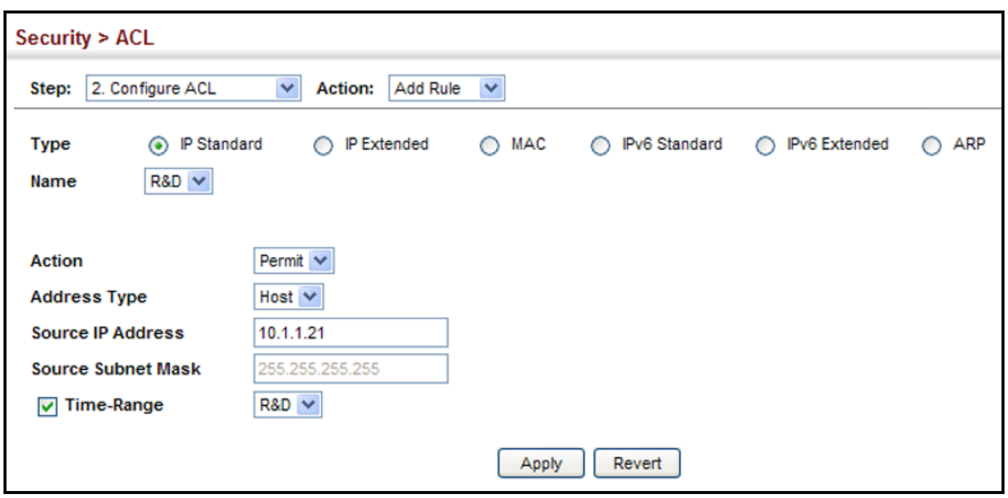
- **Time Range** – Name of a time range.

**WEB INTERFACE**

To add rules to a Standard IPv4 ACL:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Add Rule from the Action list.
4. Select IP Standard from the Type list.
5. Select the name of an ACL from the Name list.
6. Specify the action (i.e., Permit or Deny).
7. Select the address type (Any, Host, or IP).
8. If you select “Host,” enter a specific address. If you select “IP,” enter a subnet address and the mask for an address range.
9. Click Apply.

**Figure 42: Configuring a Standard IPv4 ACL**



## Configuring an Extended IPv4 ACL

Use the Security > ACL (Configure ACL - Add Rule - IP Extended) page to configure an Extended IPv4 ACL.

### CLI REFERENCES


- "permit, deny (Extended IPv4 ACL)" on page 786
- "show ip access-list" on page 789
- "Time Range" on page 654


### PARAMETERS

These parameters are displayed in the web interface:

- **Type** – Selects the type of ACLs to show in the Name list.
- **Name** – Shows the names of ACLs matching the selected type.
- **Action** – An ACL can contain any combination of permit or deny rules.
- **Source/Destination Address Type** – Specifies the source or destination IP address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and Subnet Mask fields. (Options: Any, Host, IP; Default: Any)
- **Source/Destination IP Address** – Source or destination IP address.
- **Source/Destination Subnet Mask** – Subnet mask for source or destination address. (See the description for Subnet Mask on page 281.)
- **Source/Destination Port** – Source/destination port number for the specified protocol type. (Range: 0-65535)
- **Source/Destination Port Bit Mask** – Decimal number representing the port bits to match. (Range: 0-65535)
- **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)
- **Service Type** – Packet priority settings based on the following criteria:
  - **ToS** – Type of Service level. (Range: 0-15)
  - **Precedence** – IP precedence level. (Range: 0-7)
  - **DSCP** – DSCP priority level. (Range: 0-63)
- **Control Code** – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)
- **Control Code Bit Mask** – Decimal number representing the code bits to match. (Range: 0-63)

  The control bit mask is a decimal number (for an equivalent binary bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit “1” means to match a bit and “0” means to ignore a bit. The following bits may be specified:

- 1 (fin) – Finish
- 2 (syn) – Synchronize
- 4 (rst) – Reset
- 8 (psh) – Push
- 16 (ack) – Acknowledgement
- 32 (urg) – Urgent pointer

For example, use the code value and mask below to catch packets with the following flags set:

- SYN flag valid, use control-code 2, control bit mask 2
- Both SYN and ACK valid, use control-code 18, control bit mask 18
- SYN valid and ACK invalid, use control-code 2, control bit mask 18

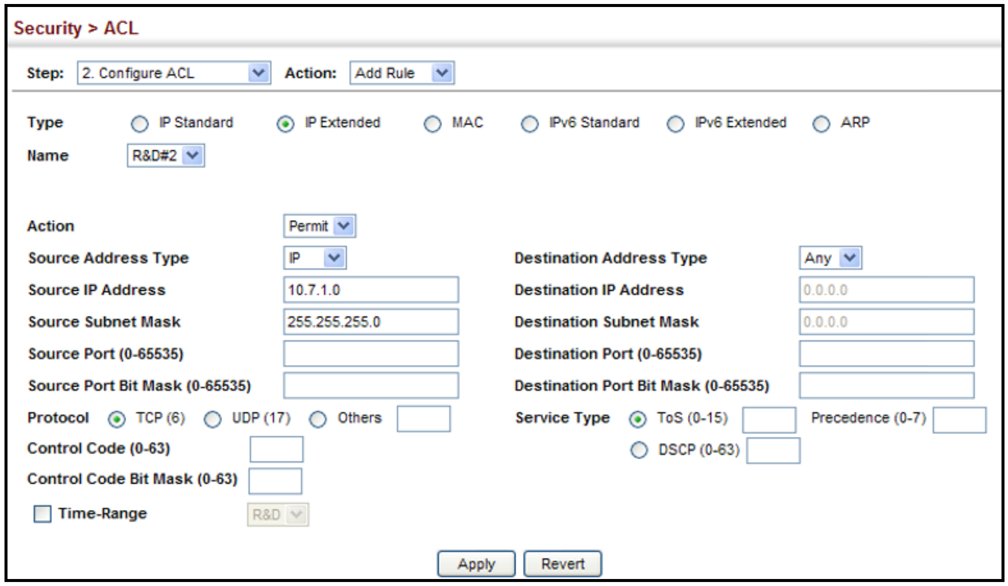
- **Time Range** – Name of a time range.

### WEB INTERFACE

To add rules to an Extended IPv4 ACL:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Add Rule from the Action list.
4. Select IP Extended from the Type list.
5. Select the name of an ACL from the Name list.
6. Specify the action (i.e., Permit or Deny).
7. Select the address type (Any, Host, or IP).
8. If you select “Host,” enter a specific address. If you select “IP,” enter a subnet address and the mask for an address range.
9. Set any other required criteria, such as service type, protocol type, or control code.
10. Click Apply.

**Figure 43: Configuring an Extended IPv4 ACL**




## Configuring a Standard IPv6 ACL

Use the Security > ACL (Configure ACL - Add Rule - IPv6 Standard) page to configure a Standard IPv6ACL.

### CLI References

- "permit, deny (Standard IPv6 ACL)" on page 791
- "show ipv6 access-list" on page 794
- "Time Range" on page 654

### Parameters

These parameters are displayed in the web interface:

- **Type** – Selects the type of ACLs to show in the Name list.
- **Name** – Shows the names of ACLs matching the selected type.
- **Action** – An ACL can contain any combination of permit or deny rules.
- **Source Address Type** – Specifies the source IP address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IPv6-prefix” to specify a range of addresses. (Options: Any, Host, IPv6-prefix; Default: Any)
- **Source IPv6 Address** – An IPv6 source address or network class. The address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- **Source Prefix-Length** – A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

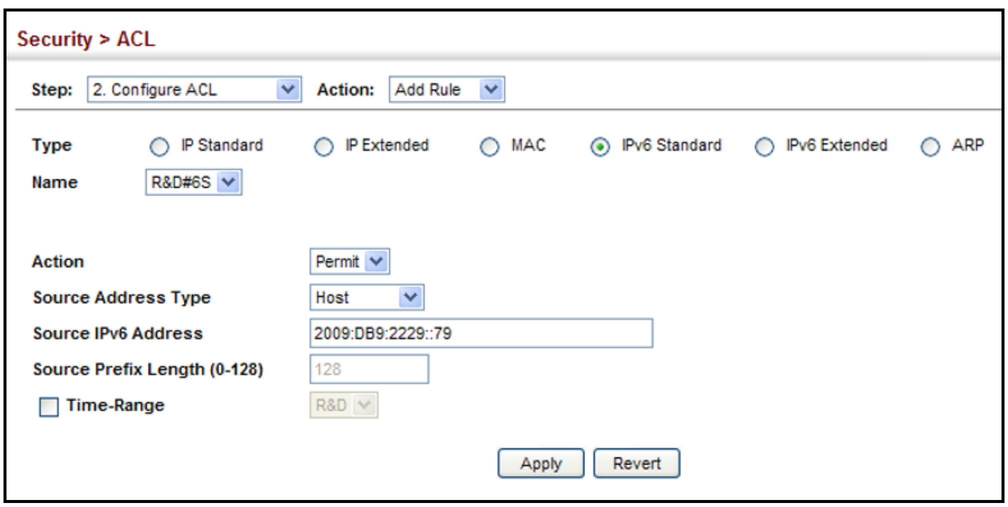
■ **Time Range** – Name of a time range.

**WEB INTERFACE**

To add rules to a Standard IPv6 ACL:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Add Rule from the Action list.
4. Select IPv6 Standard from the Type list.
5. Select the name of an ACL from the Name list.
6. Specify the action (i.e., Permit or Deny).
7. Select the source address type (Any, Host, or IPv6-prefix).
8. If you select “Host,” enter a specific address. If you select “IPv6-prefix,” enter a subnet address and the prefix length.
9. Click Apply.

**Figure 44: Configuring a Standard IPv6 ACL**



## Configuring an Extended IPv6 ACL

Use the Security > ACL (Configure ACL - Add Rule - IPv6 Extended) page to configure an Extended IPv6 ACL.

### CLI REFERENCES


- "permit, deny (Extended IPv6 ACL)" on page 792
- "show ipv6 access-list" on page 794
- "Time Range" on page 654


### PARAMETERS

These parameters are displayed in the web interface:

- **Type** – Selects the type of ACLs to show in the Name list.

- **Name** – Shows the names of ACLs matching the selected type.

- **Action** – An ACL can contain any combination of permit or deny rules.

- **Destination Address Type** – Specifies the destination IP address. Use "Any" to include all possible addresses, or "IPv6-prefix" to specify a range of addresses. (Options: Any, IPv6-prefix; Default: Any)

- **Destination IPv6 Address** – An IPv6 address or network class. The address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (The switch only checks the first 64 bits of the destination address.)

- **Destination Prefix-Length** – A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix; i.e., the network portion of the address. (Range: 0-64 bits)

- **DSCP** – DSCP traffic class. (Range: 0-63)

- **Next Header** – Identifies the type of header immediately following the IPv6 header. (Range: 0-255)

  Optional internet-layer information is encoded in separate headers that may be placed between the IPv6 header and the upper-layer header in a packet. There are a small number of such extension headers, each identified by a distinct Next Header value. IPv6 supports the values defined for the IPv4 Protocol field in RFC 1700, and includes these commonly used headers:

  0 : Hop-by-Hop Options (RFC 2460)
  6 : TCP Upper-layer Header (RFC 1700)
  17 : UDP Upper-layer Header (RFC 1700)
  43 : Routing (RFC 2460)
  44 : Fragment (RFC 2460)
  50 : Encapsulating Security Payload (RFC 2406)
  51 : Authentication (RFC 2402)
  60 : Destination Options (RFC 2460)

- **Flow Label** – A label for packets belonging to a particular traffic "flow" for which the sender requests special handling by IPv6 routers, such as non-default quality of service or "real-time" service (see RFC 2460). (Range: 0-1048575)

A flow label is assigned to a flow by the flow's source node. New flow labels must be chosen pseudo-randomly and uniformly from the range 1 to FFFFF hexadecimal. The purpose of the random allocation is to make any set of bits within the Flow Label field suitable for use as a hash key by routers, for looking up the state associated with the flow.

A flow identifies a sequence of packets sent from a particular source to a particular (unicast or multicast) destination for which the source desires special handling by the intervening routers. The nature of that special handling might be conveyed to the routers by a control protocol, such as a resource reservation protocol, or by information within the flow's packets themselves, e.g., in a hop-by-hop option. A flow is uniquely identified by the combination of a source address and a non-zero flow label. Packets that do not belong to a flow carry a flow label of zero.

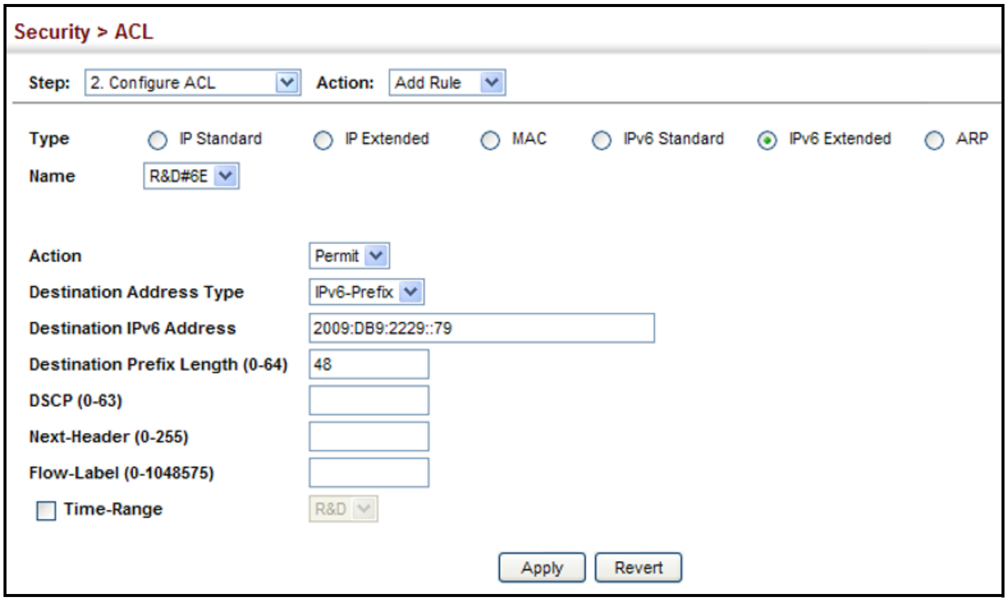
Hosts or routers that do not support the functions specified by the flow label must set the field to zero when originating a packet, pass the field on unchanged when forwarding a packet, and ignore the field when receiving a packet.

### WEB INTERFACE

To add rules to an Extended IPv6 ACL:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Add Rule from the Action list.
4. Select IPv6 Extended from the Type list.
5. Select the name of an ACL from the Name list.
6. Specify the action (i.e., Permit or Deny).
7. Select the address type (Any or IPv6-prefix).
8. If you select “Host,” enter a specific address. If you select “IPv6-prefix,” enter a subnet address and prefix length.
9. Set any other required criteria, such as DSCP, next header, or flow label.
10. Click Apply.

**Figure 45: Configuring an Extended IPv6 ACL**




## Configuring a MAC ACL

Use the Security > ACL (Configure ACL - Add Rule - MAC) page to configure a MAC ACL based on hardware addresses, packet format, and Ethernet type.

### CLI REFERENCES

- "permit, deny (MAC ACL)" on page 797
- "show ip access-list" on page 789
- "Time Range" on page 654

### PARAMETERS

These parameters are displayed in the web interface:

- **Type** – Selects the type of ACLs to show in the Name list.
- **Name** – Shows the names of ACLs matching the selected type.
- **Action** – An ACL can contain any combination of permit or deny rules.
- **Source/Destination Address Type** – Use "Any" to include all possible addresses, "Host" to indicate a specific MAC address, or "MAC" to specify an address range with the Address and Bit Mask fields. (Options: Any, Host, MAC; Default: Any)
- **Source/Destination MAC Address** – Source or destination MAC address.
- **Source/Destination Bit Mask** – Hexadecimal mask for source or destination MAC address.
- **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.

■**VID** – VLAN ID. (Range: 1-4095)

■**VID Bit Mask** – VLAN bit mask. (Range: 0-4095)

■**Ethernet Type** – This option can only be used to filter Ethernet II formatted packets. (Range: 600-ffff hex.)

A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX).

■**Ethernet Type Bit Mask** – Protocol bit mask. (Range: 600-ffff hex.)

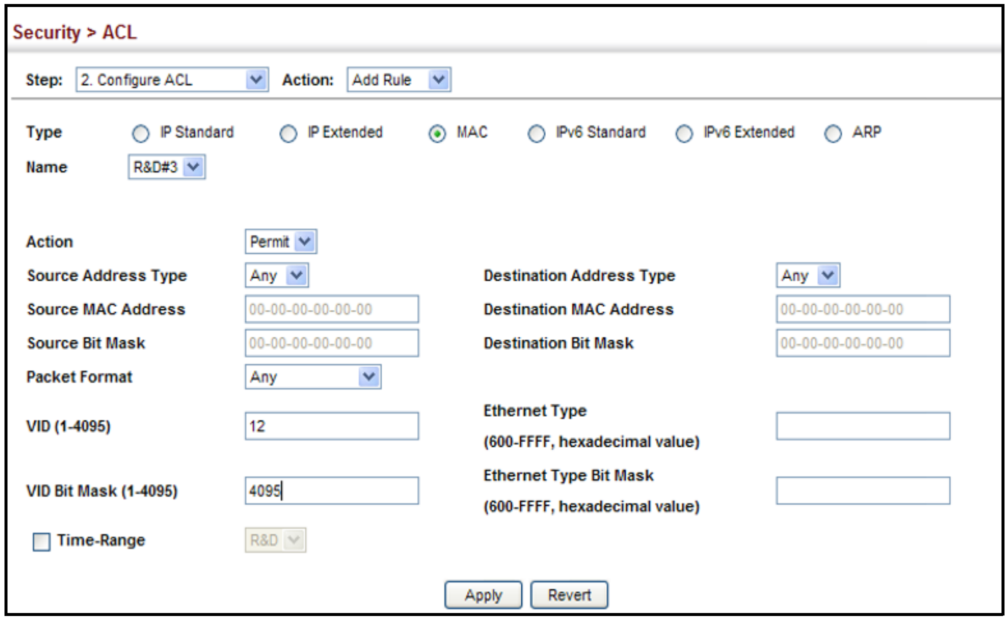
■**Time Range** – Name of a time range.

**WEB INTERFACE**

To add rules to a MAC ACL:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Add Rule from the Action list.
4. Select MAC from the Type list.
5. Select the name of an ACL from the Name list.
6. Specify the action (i.e., Permit or Deny).
7. Select the address type (Any, Host, or MAC).
8. If you select “Host,” enter a specific address (e.g., 11-22-33-44-55-66). If you select “MAC,” enter a base address and a hexadecimal bit mask for an address range.
9. Set any other required criteria, such as VID, Ethernet type, or packet format.
10. Click Apply.

**Figure 46: Configuring a MAC ACL**




## Configuring an ARP ACL

Use the Security > ACL (Configure ACL - Add Rule - ARP) page to configure ACLs based on ARP message addresses. ARP Inspection can then use these ACLs to filter suspicious traffic (see "Configuring Global Settings for ARP Inspection" on page 295).

### CLI REFERENCES

- "permit, deny (ARP ACL)" on page 802
- "show ip access-list" on page 789
- "Time Range" on page 654

### PARAMETERS

These parameters are displayed in the web interface:

- **Type** – Selects the type of ACLs to show in the Name list.

- **Name** – Shows the names of ACLs matching the selected type.

- **Action** – An ACL can contain any combination of permit or deny rules.

- **Packet Type** – Indicates an ARP request, ARP response, or either type. (Range: Request, Response, All; Default: Request)

- **Source/Destination IP Address Type** – Specifies the source or destination IPv4 address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and Mask fields. (Options: Any, Host, IP; Default: Any)

- **Source/Destination IP Address** – Source or destination IP address.

- **Source/Destination IP Subnet Mask** – Subnet mask for source or destination address. (See the description for Subnet Mask on page 281.)

■**Source/Destination MAC Address Type** – Use “Any” to include all possible addresses, “Host” to indicate a specific MAC address, or “MAC” to specify an address range with the Address and Mask fields. (Options: Any, Host, MAC; Default: Any)

■**Source/Destination MAC Address** – Source or destination MAC address.

■**Source/Destination MAC Bit Mask** – Hexadecimal mask for source or destination MAC address.

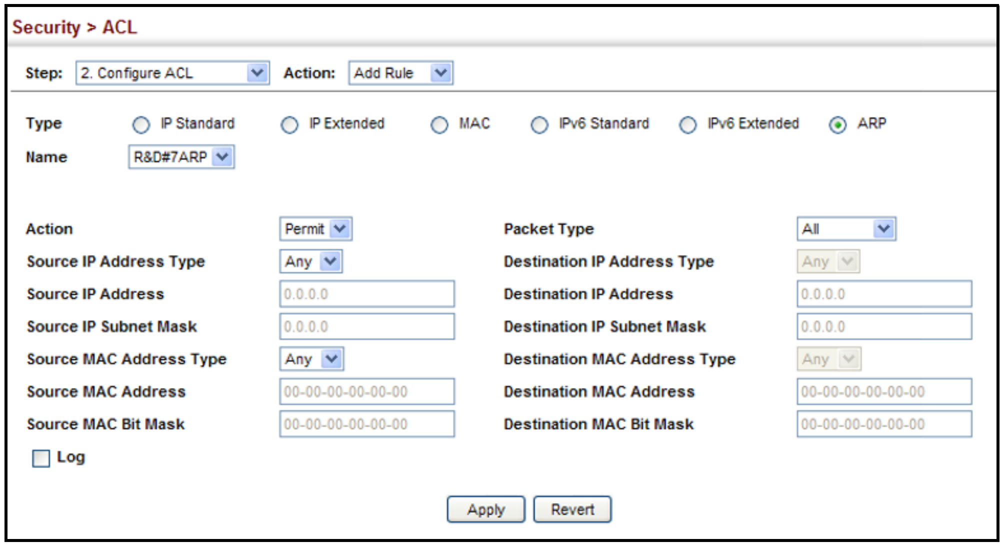
■**Log** – Logs a packet when it matches the access control entry.

**WEB INTERFACE**

To add rules to an ARP ACL:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Add Rule from the Action list.
4. Select ARP from the Type list.
5. Select the name of an ACL from the Name list.
6. Specify the action (i.e., Permit or Deny).
7. Select the packet type (Request, Response, All).
8. Select the address type (Any, Host, or IP).
9. If you select “Host,” enter a specific address (e.g., 11-22-33-44-55-66). If you select “IP,” enter a base address and a hexadecimal bit mask for an address range.
10. Enable logging if required.
11. Click Apply.

**Figure 47: Configuring a ARP ACL**




## Binding a Port to an Access Control List

After configuring ACLs, use the Security > ACL (Configure Interface) page to bind the ports that need to filter traffic to the appropriate ACLs. You can assign one IP access list and one MAC access list to any port.

### CLI REFERENCES

■"ip access-group" on page 788
■"ipv6 access-group" on page 794
■"show ip access-group" on page 789
■"show ipv6 access-group" on page 795
■"mac access-group" on page 799
■"show mac access-group" on page 800
■"Time Range" on page 654

### COMMAND USAGE

■This switch supports ACLs for ingress filtering only.

■You only bind one ACL to any port for ingress filtering.

### PARAMETERS

These parameters are displayed in the web interface:

■**Type** – Selects the type of ACLs to bind to a port.

■**Port** – Port identifier

■**ACL** – ACL used for ingress packets.

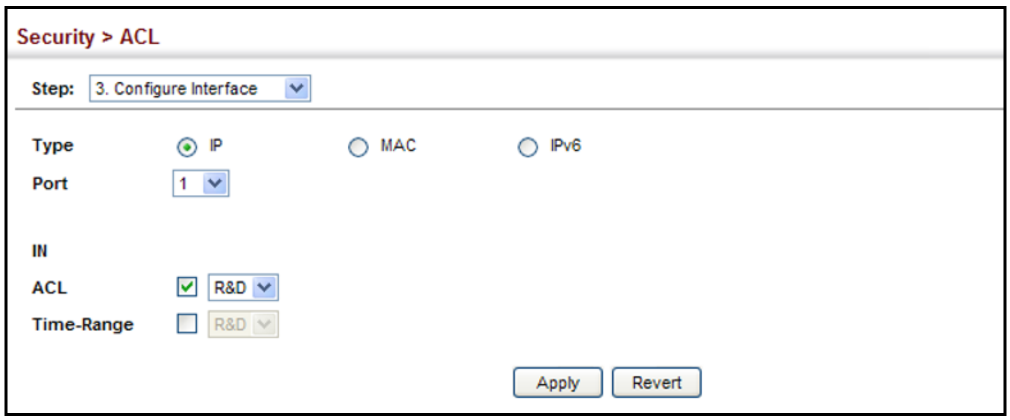
■**Time Range** – Name of a time range.

**WEB INTERFACE**

To bind an ACL to a port:

1. Click Security, ACL.
2. Select Configure Interface from the Step list.
3. Select IP or MAC from the Type list.
4. Select the name of an ACL from the ACL list.
5. Click Apply.

**Figure 48: Binding a Port to an ACL**




## ARP INSPECTION

ARP Inspection is a security feature that validates the MAC Address bindings for Address Resolution Protocol packets. It provides protection against ARP traffic with invalid MAC-to-IP address bindings, which forms the basis for certain “man-in-the-middle” attacks. This is accomplished by intercepting all ARP requests and responses and verifying each of these packets before the local ARP cache is updated or the packet is forwarded to the appropriate destination. Invalid ARP packets are dropped.

ARP Inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database – the DHCP snooping binding database (see "DHCP Snooping Configuration" on page 320). This database is built by DHCP snooping if it is enabled on globally on the switch and on the required VLANs. ARP Inspection can also validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured addresses (see "Configuring an ARP ACL" on page 291).

**COMMAND USAGE**

*Enabling & Disabling ARP Inspection*

■ARP Inspection is controlled on a global and VLAN basis.

- By default, ARP Inspection is disabled both globally and on all VLANs.
  - If ARP Inspection is globally enabled, then it becomes active only on the VLANs where it has been enabled.
  - When ARP Inspection is enabled globally, all ARP request and reply packets on inspection-enabled VLANs are redirected to the CPU and their switching behavior handled by the ARP Inspection engine.
  - If ARP Inspection is disabled globally, then it becomes inactive for all VLANs, including those where inspection is enabled.
  - When ARP Inspection is disabled, all ARP request and reply packets will bypass the ARP Inspection engine and their switching behavior will match that of all other packets.
  - Disabling and then re-enabling global ARP Inspection will not affect the ARP Inspection configuration of any VLANs.
  - When ARP Inspection is disabled globally, it is still possible to configure ARP Inspection for individual VLANs. These configuration changes will only become active after ARP Inspection is enabled globally again.
- The ARP Inspection engine in the current firmware version does not support ARP Inspection on trunk ports.

## Configuring Global Settings for ARP Inspection

Use the Security > ARP Inspection (Configure General) page to enable ARP inspection globally for the switch, to validate address information in each packet, and configure logging.

### CLI REFERENCES

- "ARP Inspection" on page 773

### COMMAND USAGE

*ARP Inspection Validation*

- By default, ARP Inspection Validation is disabled.
- Specifying at least one of the following validations enables ARP Inspection Validation globally. Any combination of the following checks can be active concurrently.
  - Destination MAC – Checks the destination MAC address in the Ethernet header against the target MAC address in the ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.
  - IP – Checks the ARP body for invalid and unexpected IP addresses. These addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, while target IP addresses are checked only in ARP responses.

- Source MAC – Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

*ARP Inspection Logging*

- By default, logging is active for ARP Inspection, and cannot be disabled.
- The administrator can configure the log facility rate.
- When the switch drops a packet, it places an entry in the log buffer, then generates a system message on a rate-controlled basis. After the system message is generated, the entry is cleared from the log buffer.
- Each log entry contains flow information, such as the receiving VLAN, the port number, the source and destination IP addresses, and the source and destination MAC addresses.
- If multiple, identical invalid ARP packets are received consecutively on the same VLAN, then the logging facility will only generate one entry in the log buffer and one corresponding system message.
- If the log buffer is full, the oldest entry will be replaced with the newest entry.

**PARAMETERS**

These parameters are displayed in the web interface:

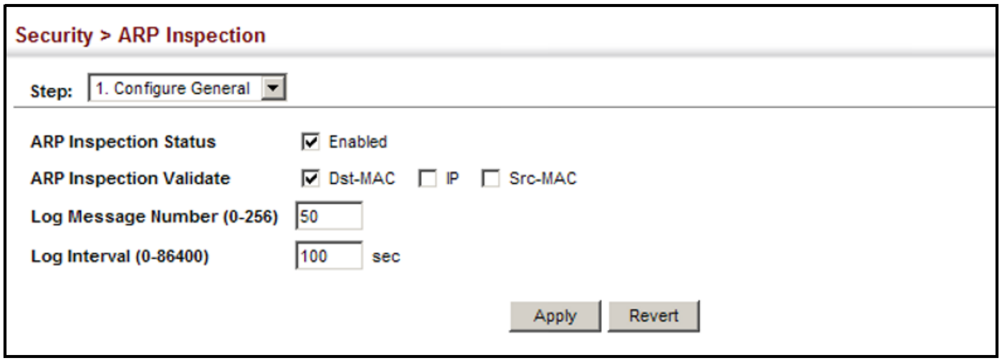
- **ARP Inspection Status** – Enables ARP Inspection globally. (Default: Disabled)
- **ARP Inspection Validation** – Enables extended ARP Inspection Validation if any of the following options are enabled. (Default: Disabled)
  - **Dst-MAC** – Validates the destination MAC address in the Ethernet header against the target MAC address in the body of ARP responses.
  - **IP** – Checks the ARP body for invalid and unexpected IP addresses. Sender IP addresses are checked in all ARP requests and responses, while target IP addresses are checked only in ARP responses.
  - **Src-MAC** – Validates the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses.
- **Log Message Number** – The maximum number of entries saved in a log message. (Range: 0-256; Default: 5)
- **Log Interval** – The interval at which log messages are sent. (Range: 0-86400 seconds; Default: 1 second)

### WEB INTERFACE

To configure global settings for ARP Inspection:

1. Click Security, ARP Inspection.
2. Select Configure General from the Step list.
3. Enable ARP inspection globally, enable any of the address validation options, and adjust any of the logging parameters if required.
4. Click Apply.

**Figure 49: Configuring Global Settings for ARP Inspection**




## Configuring VLAN Settings for ARP Inspection

Use the Security > ARP Inspection (Configure VLAN) page to enable ARP inspection for any VLAN and to specify the ARP ACL to use.

### CLI REFERENCES

■"ARP Inspection" on page 773

### COMMAND USAGE

*ARP Inspection VLAN Filters (ACLs)*

■By default, no ARP Inspection ACLs are configured and the feature is disabled.

■ARP Inspection ACLs are configured within the ARP ACL configuration page (see page 291).

■ARP Inspection ACLs can be applied to any configured VLAN.

■ARP Inspection uses the DHCP snooping bindings database for the list of valid IP-to-MAC address bindings. ARP ACLs take precedence over entries in the DHCP snooping bindings database. The switch first compares ARP packets to any specified ARP ACLs.

■If *Static* is specified, ARP packets are only validated against the selected ACL – packets are filtered according to any matching rules, packets not matching any rules are dropped, and the DHCP snooping bindings database check is bypassed.

- If *Static* is not specified, ARP packets are first validated against the selected ACL; if no ACL rules match the packets, then the DHCP snooping bindings database determines their validity.

### PARAMETERS

These parameters are displayed in the web interface:

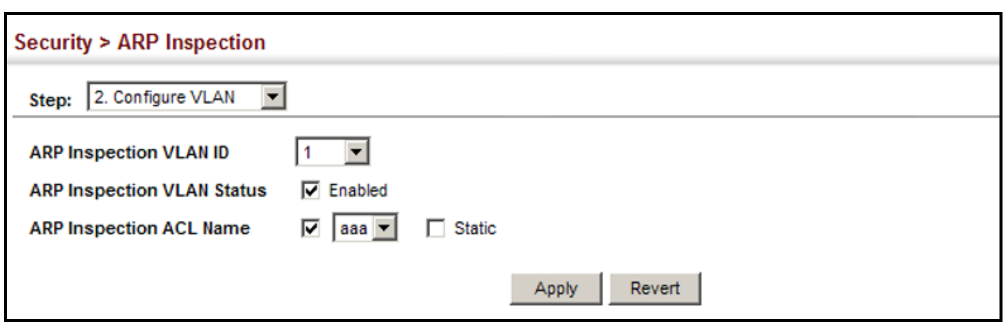
- **ARP Inspection VLAN ID** – Selects any configured VLAN. (Default: 1)
- **ARP Inspection VLAN Status** – Enables ARP Inspection for the selected VLAN. (Default: Disabled)
- **ARP Inspection ACL Name**
  - *ARP ACL* – Allows selection of any configured ARP ACLs. (Default: None)
  - **Static** – When an ARP ACL is selected, and static mode also selected, the switch only performs ARP Inspection and bypasses validation against the DHCP Snooping Bindings database. When an ARP ACL is selected, but static mode is not selected, the switch first performs ARP Inspection and then validation against the DHCP Snooping Bindings database. (Default: Disabled)

### WEB INTERFACE

To configure VLAN settings for ARP Inspection:

1. Click Security, ARP Inspection.
2. Select Configure VLAN from the Step list.
3. Enable ARP inspection for the required VLANs, select an ARP ACL filter to check for configured addresses, and select the Static option to bypass checking the DHCP snooping bindings database if required.
4. Click Apply.

**Figure 50: Configuring VLAN Settings for ARP Inspection**




## Configuring Interface Settings for ARP Inspection

Use the Security > ARP Inspection (Configure Interface) page to specify the ports that require ARP inspection, and to adjust the packet inspection rate.

### CLI REFERENCES

■ "ARP Inspection" on page 773

### PARAMETERS

These parameters are displayed in the web interface:

■ **Port** – Port identifier.

■ **Trust Status** – Configures the port as trusted or untrusted. (Default: Untrusted)

By default, all untrusted ports are subject to ARP packet rate limiting, and all trusted ports are exempt from ARP packet rate limiting.

Packets arriving on trusted interfaces bypass all ARP Inspection and ARP Inspection Validation checks and will always be forwarded, while those arriving on untrusted interfaces are subject to all configured ARP inspection tests.

■ **Packet Rate Limit** – Sets the maximum number of ARP packets that can be processed by CPU per second on untrusted ports.
(Range: 0-2048; Default: 15)

Setting the rate limit to “0” means that there is no restriction on the number of ARP packets that can be processed by the CPU.

The switch will drop all ARP packets received on a port which exceeds the configured ARP-packets-per-second rate limit.

### WEB INTERFACE

To configure interface settings for ARP Inspection:

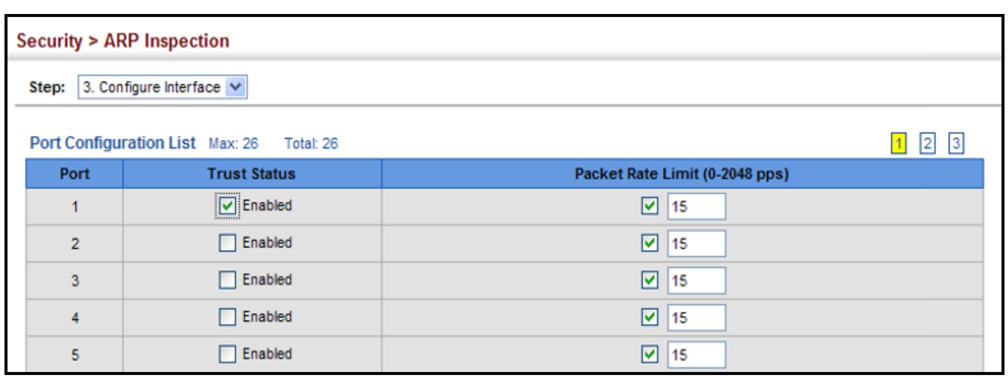
1. Click Security, ARP Inspection.

2. Select Configure Interface from the Step list.

3. Specify any untrusted ports which require ARP inspection, and adjust the packet inspection rate.

4. Click Apply.

**Figure 51: Configuring Interface Settings for ARP Inspection**



## Displaying ARP Inspection Statistics

Use the Security > ARP Inspection (Show Information - Show Statistics) page to display statistics about the number of ARP packets processed, or dropped for various reasons.

### CLI References

■ "show ip arp inspection statistics" on page 781

### Parameters

These parameters are displayed in the web interface:

**Table 3: ARP Inspection Statistics**

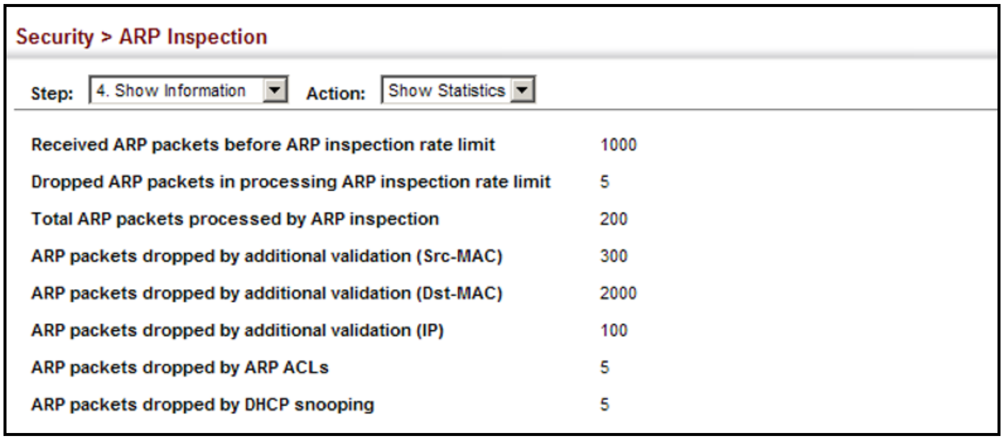
| Parameter | Description |
|---|---|
| Received ARP packets before ARP inspection rate limit | Count of ARP packets received but not exceeding the ARP Inspection rate limit. |
| Dropped ARP packets in the process of ARP inspection rate limit | Count of ARP packets exceeding (and dropped by) ARP rate limiting. |
| ARP packets dropped by additional validation (IP) | Count of ARP packets that failed the IP address test. |
| ARP packets dropped by additional validation (Dst-MAC) | Count of packets that failed the destination MAC address test. |
| Total ARP packets processed by ARP inspection | Count of all ARP packets processed by the ARP Inspection engine. |
| ARP packets dropped by additional validation (Src-MAC) | Count of packets that failed the source MAC address test. |
| ARP packets dropped by ARP ACLs | Count of ARP packets that failed validation against ARP ACL rules. |
| ARP packets dropped by DHCP snooping | Count of packets that failed validation against the DHCP Snooping Binding database. |

### Web Interface

To display statistics for ARP Inspection:

1. Click Security, ARP Inspection.
2. Select Show Information from the Step list.
3. Select Show Statistics from the Step list.

**Figure 52: Displaying Statistics for ARP Inspection**




## Displaying the ARP Inspection Log

Use the Security > ARP Inspection (Show Information - Show Log) page to show information about entries stored in the log, including the associated VLAN, port, and address components.

### CLI References

■ "show ip arp inspection log" on page 780

### Parameters

These parameters are displayed in the web interface:

**Table 4: ARP Inspection Log**

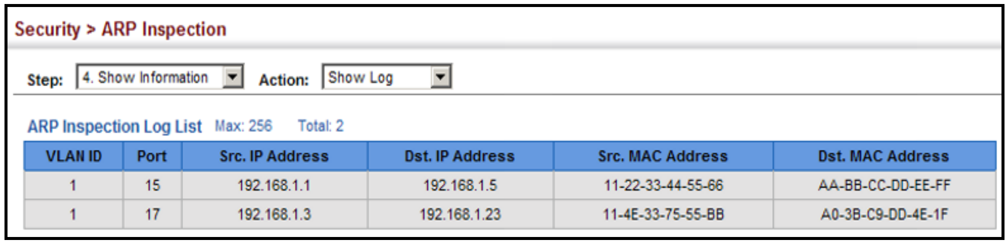
| Parameter | Description |
|---|---|
| VLAN ID | The VLAN where this packet was seen. |
| Port | The port where this packet was seen. |
| Src. IP Address | The source IP address in the packet. |
| Dst. IP Address | The destination IP address in the packet. |
| Src. MAC Address | The source MAC address in the packet. |
| Dst. MAC Address | The destination MAC address in the packet. |

### Web Interface

To display the ARP Inspection log:

1. Click Security, ARP Inspection.
2. Select Show Information from the Step list.
3. Select Show Log from the Step list.

**Figure 53: Displaying the ARP Inspection Log**




## FILTERING IP ADDRESSES FOR MANAGEMENT ACCESS

Use the Security > IP Filter page to create a list of up to 15 IP addresses or IP address groups that are allowed management access to the switch through the web interface, SNMP, or Telnet.

### CLI REFERENCES

- "Management IP Filter" on page 735

### COMMAND USAGE

- The management interfaces are open to all IP addresses by default. Once you add an entry to a filter list, access to that interface is restricted to the specified addresses.
- If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- IP address can be configured for SNMP, web and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.
- When entering addresses for the same group (i.e., SNMP, web or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.
- You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.
- You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

### PARAMETERS

These parameters are displayed in the web interface:

- **Mode**
  - **Web** – Configures IP address(es) for the web group.
  - **SNMP** – Configures IP address(es) for the SNMP group.

◆ **Telnet** – Configures IP address(es) for the Telnet group.

■ **Start IP Address** – A single IP address, or the starting address of a range.

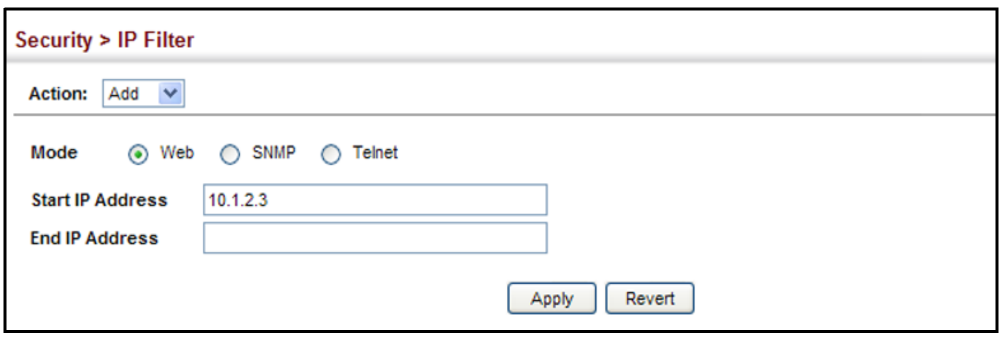
■ **End IP Address** – The end address of a range.

### WEB INTERFACE

To create a list of IP addresses authorized for management access:

1. Click Security, IP Filter.
2. Select Add from the Action list.
3. Select the management interface to filter (Web, SNMP, Telnet).
4. Enter the IP addresses or range of addresses that are allowed management access to an interface.
5. Click Apply

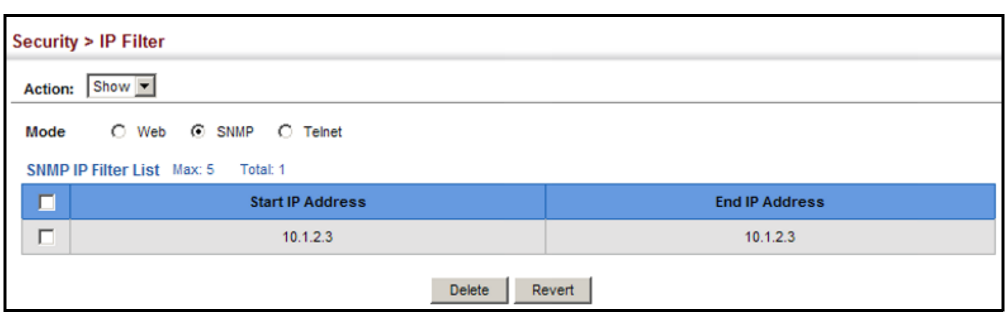
**Figure 54: Creating an IP Address Filter for Management Access**




To show a list of IP addresses authorized for management access:

1. Click Security, IP Filter.
2. Select Show from the Action list.

**Figure 55: Showing IP Addresses Authorized for Management Access**



## CONFIGURING PORT SECURITY

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

When port security is enabled on a port, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be authorized to access the network through that port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

To use port security, specify a maximum number of addresses to allow on the port and then let the switch dynamically learn the <source MAC address, VLAN> pair for frames received on the port. Note that you can also manually add secure addresses to the port using the Static Address Table (page 170). When the port has reached the maximum number of MAC addresses, the selected port will stop learning. The MAC addresses already in the address table will be retained and will not age out. Any other device that attempts to use the port will be prevented from accessing the switch.

### CLI REFERENCES

■"Port Security" on page 740

### COMMAND USAGE

■A secure port has the following restrictions:

- It cannot be used as a member of a static or dynamic trunk.
- It should not be connected to a network interconnection device.

■The default maximum number of MAC addresses allowed on a secure port is zero. You must configure a maximum address count from 1-1024 for the port to allow access.

■If a port is disabled (shut down) due to a security violation, it must be manually re-enabled from the Interface > Port > General page (page 107).

### PARAMETERS

These parameters are displayed in the web interface:

■**Port** – Port number.

■**Action** – Indicates the action to be taken when a port security violation is detected:

- **None**: No action should be taken. (This is the default.)
- **Trap**: Send an SNMP trap message.
- **Shutdown**: Disable the port.
- **Trap and Shutdown**: Send an SNMP trap message and disable the port.

■**Security Status** – Enables or disables port security on the port. (Default: Disabled)

■**Max MAC Count** – The maximum number of MAC addresses that can be learned on a port. (Range: 0-1024, where 0 means disabled)

The maximum address count is effective when port security is enabled or disabled, but can only be set when Security Status is disabled.

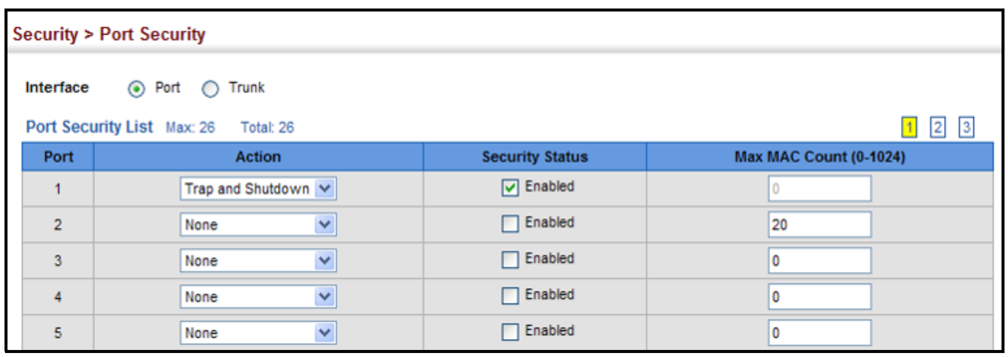
**WEB INTERFACE**
To configure port security:

1. Click Security, Port Security.

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

3. Click Apply

**Figure 56: Configuring Port Security**



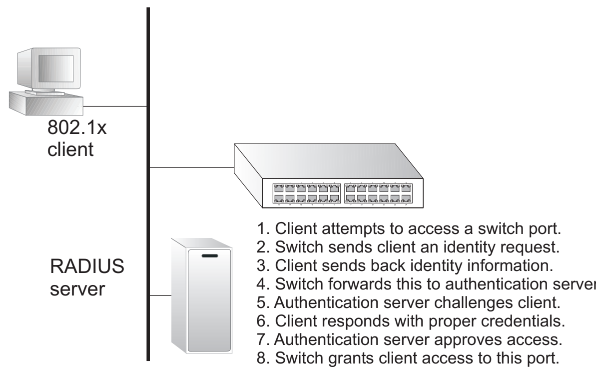

## CONFIGURING 802.1X PORT AUTHENTICATION

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

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

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

**Figure 57:  Configuring Port Security**




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

- The switch must have an IP address assigned.
- RADIUS authentication must be enabled on the switch and the IP address of the RADIUS server specified.
- 802.1X must be enabled globally for the switch.
- Each switch port that will be used must be set to dot1X “Auto” mode.
- Each client that needs to be authenticated must have dot1X client software installed and properly configured.
- The RADIUS server and 802.1X client support EAP. (The switch only supports EAPOL in order to pass the EAP packets from the server to the client.)
- The RADIUS server and client also have to support the same EAP authentication type – MD5, PEAP, TLS, or TTLS. (Native support for these encryption methods is provided in Windows XP, and in Windows 2000 with Service Pack 4. To support these encryption methods in Windows 95 and 98, you can use the AEGIS dot1x client or other comparable client software)

## Configuring 802.1X Global Settings

Use the Security > Port Authentication (Configure Global) page to configure IEEE 802.1X port authentication. The 802.1X protocol must be enabled globally for the switch system before port settings are active.

### CLI REFERENCES

- "802.1X Port Authentication" on page 725

### PARAMETERS

These parameters are displayed in the web interface:

- **Port Authentication Status** – Sets the global setting for 802.1X. (Default: Disabled)
- **EAPOL Pass Through** – Passes EAPOL frames through to all ports in STP forwarding state when dot1x is globally disabled. (Default: Disabled)

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

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

### WEB INTERFACE

To configure global settings for 802.1X:

1. Click Security, Port Authentication.
2. Select Configure Global from the Step list.
3. Enable 802.1X globally for the switch, and configure EAPOL Pass Through if required. Then set the user name and password to use when the switch responds an MD5 challenge from the authentication server.
4. Click Apply

**Figure 58: Configuring Global Settings for 802.1X Port Authentication**

## Configuring Port Settings for 802.1X

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

### CLI REFERENCES

■"802.1X Port Authentication" on page 725

### COMMAND USAGE

When the switch functions as a local authenticator between supplicant devices attached to the switch and the authentication server, configure the parameters for the exchange of EAP messages between the authenticator and clients.

### PARAMETERS

These parameters are displayed in the web interface:

- **Port** – Port number.
- **Status** – Indicates if authentication is enabled or disabled on the port. The status is disabled if the control mode is set to Force-Authorized.
- **Authorized** – Displays the 802.1X authorization status of connected clients.
  - **Yes** – Connected client is authorized.
  - **No** – Connected client is not authorized.
- **Supplicant** – Indicates the MAC address of a connected client.
- **Control 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.
- **Operation Mode** – Allows single or multiple hosts (clients) to connect to an 802.1X-authorized port. (Default: Single-Host)
  - **Single-Host** – Allows only a single host to connect to this port.
  - **Multi-Host** – Allows multiple host to connect to this port.

    In this mode, only one host connected to a port needs to pass authentication for all other hosts to be granted network access. Similarly, a port can become unauthorized for all hosts if one attached host fails re-authentication or sends an EAPOL logoff message.

- **MAC-Based** – Allows multiple hosts to connect to this port, with each host needing to be authenticated.

  In this mode, each host connected to a port needs to pass authentication. The number of hosts allowed access to a port operating in this mode is limited only by the available space in the secure address table (i.e., up to 1024 addresses).

- **Max MAC Count** – The maximum number of hosts that can connect to a port when the Multi-Host operation mode is selected. (Range: 1-1024; Default: 5)

- **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)

- **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)

- **Supplicant Timeout** – Sets the time that a switch port waits for a response to an EAP request from a client before re-transmitting an EAP packet. (Range: 1-65535; Default: 30 seconds)

  This command attribute sets the timeout for EAP-request frames other than EAP-request/identity frames. If dot1x authentication is enabled on a port, the switch will initiate authentication when the port link state comes up. It will send an EAP-request/identity frame to the client to request its identity, followed by one or more requests for authentication information. It may also send other EAP-request frames to the client during an active connection as required for reauthentication.

- **Server Timeout** – Sets the time that a switch port waits for a response to an EAP request from an authentication server before re-transmitting an EAP packet. (Fixed Setting: 10 seconds)

- **Re-authentication Status** – 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)

- **Re-authentication Period** – Sets the time period after which a connected client must be re-authenticated. (Range: 1-65535 seconds; Default: 3600 seconds)

- **Intrusion Action** – Sets the port's response to a failed authentication.

  - **Block Traffic** – Blocks all non-EAP traffic on the port. (This is the default setting.)

  - **Guest VLAN** – All traffic for the port is assigned to a guest VLAN. The guest VLAN must be separately configured (See "Configuring VLAN Groups" on page 140) and mapped on each port (See "Configuring Network Access for Ports" on page 259).

*Authenticator PAE State Machine*

- **State** – Current state (including initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized).
- **Reauth Count** – Number of times connecting state is re-entered.
- **Current Identifier** – Identifier sent in each EAP Success, Failure or Request packet by the Authentication Server.

*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*

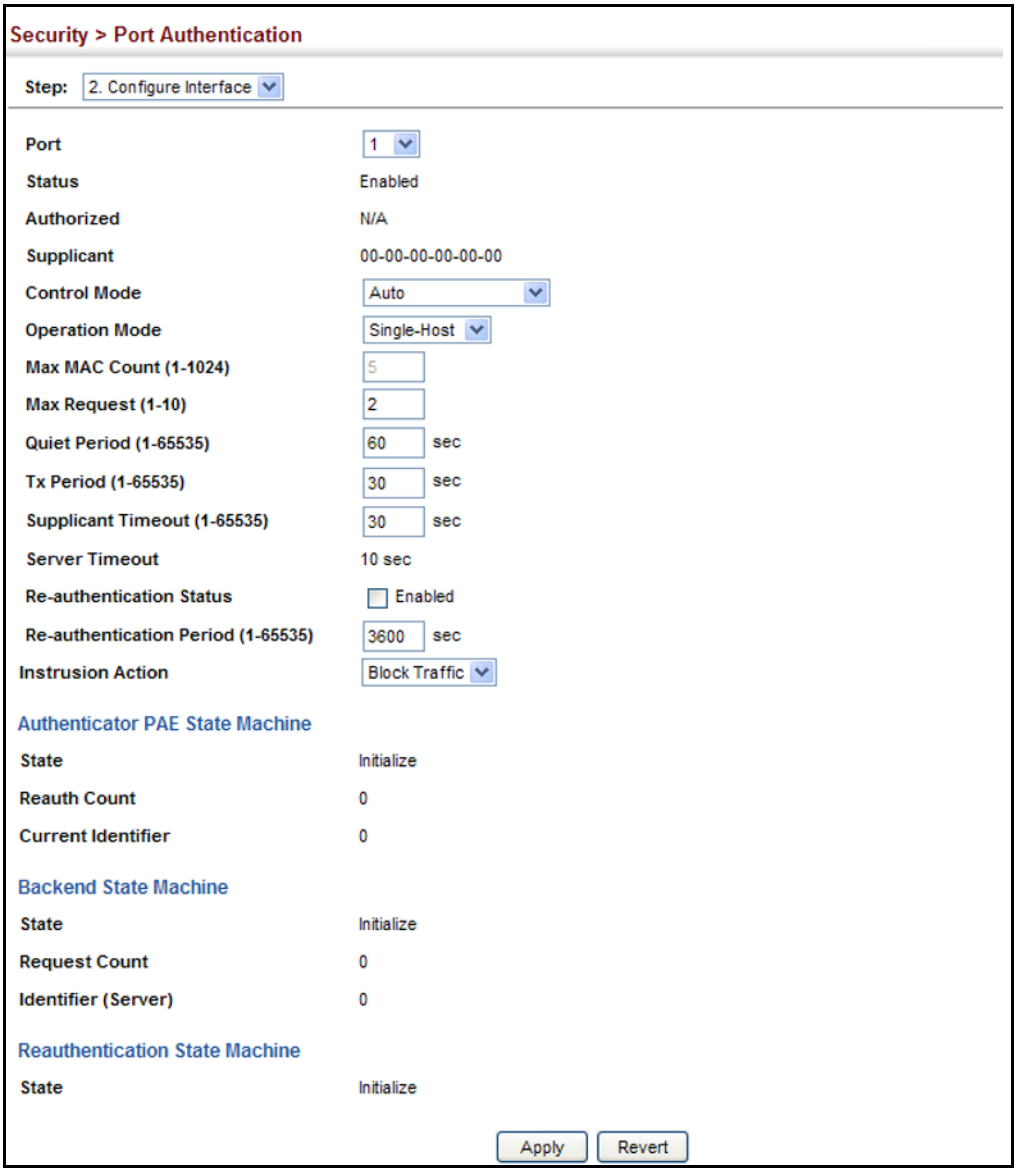
- **State** – Current state (including initialize, reauthenticate).

**WEB INTERFACE**

To configure port authenticator settings for 802.1X:

1. Click Security, Port Authentication.
2. Select Configure Interface from the Step list.
3. Click Authenticator.
4. Modify the authentication settings for each port as required.
5. Click Apply

**Figure 59: Configuring Interface Settings for 802.1X Port Authenticator**



## Displaying 802.1X Statistics

Use the Security > Port Authentication (Show Statistics) page to display statistics for dot1x protocol exchanges for any port.

### CLI REFERENCES

■ "show dot1x" on page 733

### PARAMETERS

These parameters are displayed in the web interface:

**Table 5: 802.1X Statistics**

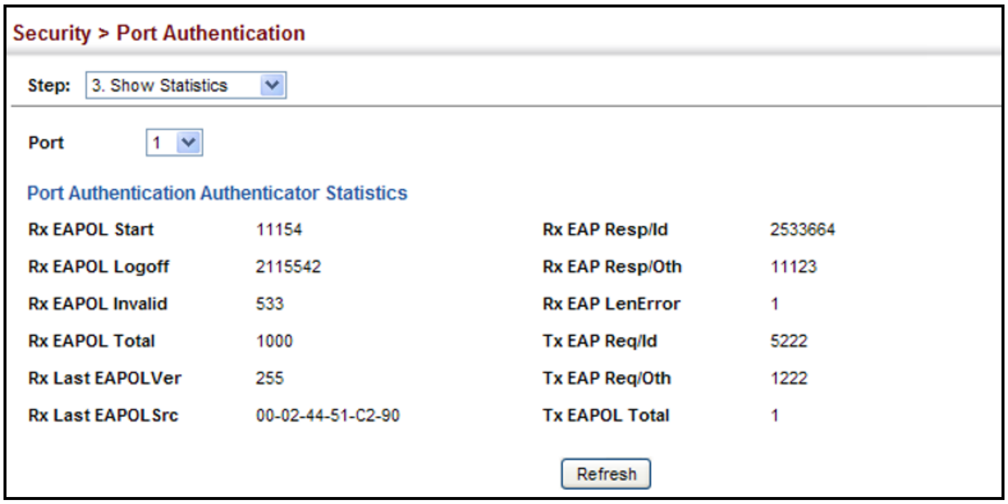
| Parameter | Description |
|---|---|
| Rx EAPOL Start | The number of EAPOL Start frames that have been received by this Authenticator. |
| Rx EAPOL Logoff | The number of EAPOL Logoff frames that have been received by this Authenticator. |
| Rx EAPOL Invalid | The number of EAPOL frames that have been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

### WEB INTERFACE

To display port authenticator statistics for 802.1X:

1. Click Security, Port Authentication.
2. Select Show Statistics from the Step list.
3. Click Authenticator.

**Figure 60: Showing Statistics for 802.1X Port Authenticator**




## IP SOURCE GUARD

IP Source Guard is a security feature that filters IP traffic on network interfaces based on manually configured entries in the IP Source Guard table, or dynamic entries in the DHCP Snooping table when enabled (see "DHCP Snooping" on page 318). IP source guard can be used to prevent traffic attacks caused when a host tries to use the IP address of a neighbor to access the network. This section describes commands used to configure IP Source Guard.

### Configuring Ports for IP Source Guard

Use the Security > IP Source Guard > Port Configuration page to set the filtering type based on source IP address, or source IP address and MAC address pairs.

IP Source Guard is used to filter traffic on an insecure port which receives messages from outside the network or fire wall, and therefore may be subject to traffic attacks caused by a host trying to use the IP address of a neighbor.

### CLI REFERENCES

- "ip source-guard" on page 770

### COMMAND USAGE

- Setting source guard mode to SIP (Source IP) or SIP-MAC (Source IP and MAC) enables this function on the selected port. Use the SIP option to check the VLAN ID, source IP address, and port number against all entries in the binding table.

Use the SIP-MAC option to check these same parameters, plus the source MAC address. If no matching entry is found, the packet is dropped.

**NOTE:** Multicast addresses cannot be used by IP Source Guard.

- When enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping (see "DHCP Snooping" on page 318), or static addresses configured in the source guard binding table.
- If IP source guard is enabled, an inbound packet's IP address (SIP option) or both its IP address and corresponding MAC address (SIP-MAC option) will be checked against the binding table. If no matching entry is found, the packet will be dropped.
- Filtering rules are implemented as follows:
  - If DHCP snooping is disabled (see page 320), IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the SIP-MAC option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, the packet will be forwarded.
  - If DHCP snooping is enabled, IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the SIP-MAC option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, or dynamic DHCP snooping binding, the packet will be forwarded.
  - If IP source guard if enabled on an interface for which IP source bindings have not yet been configured (neither by static configuration in the IP source guard binding table nor dynamically learned from DHCP snooping), the switch will drop all IP traffic on that port, except for DHCP packets.

**PARAMETERS**

These parameters are displayed in the web interface:

- **Filter Type** – Configures the switch to filter inbound traffic based source IP address, or source IP address and corresponding MAC address. (Default: None)
  - **None** – Disables IP source guard filtering on the port.
  - **SIP** – Enables traffic filtering based on IP addresses stored in the binding table.
  - **SIP-MAC** – Enables traffic filtering based on IP addresses and corresponding MAC addresses stored in the binding table.
- **Max Binding Entry** – The maximum number of entries that can be bound to an interface. (Range: 1-5; Default: 5)

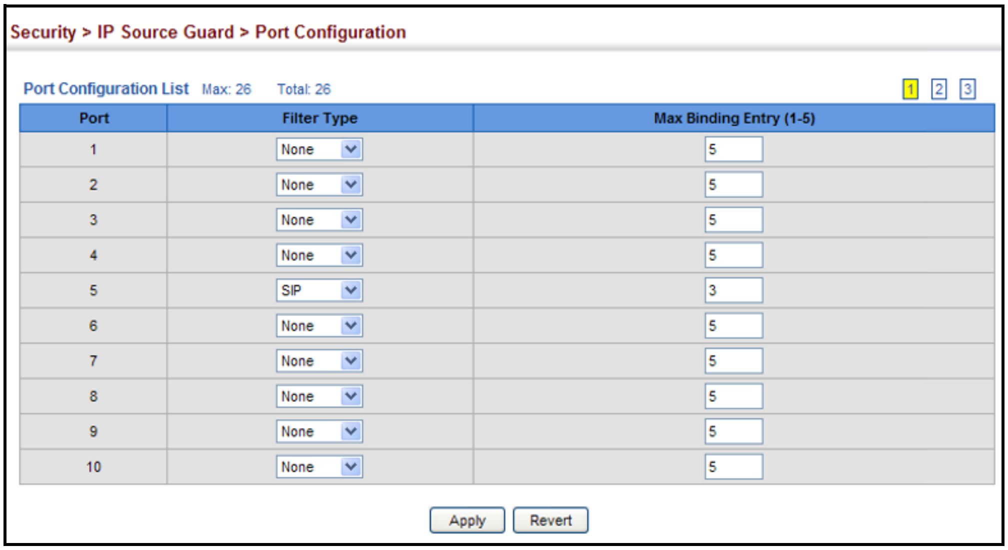
  This parameter sets the maximum number of address entries that can be mapped to an interface in the binding table, including both dynamic entries discovered by DHCP snooping (see "DHCP Snooping" on page 318) and static entries set by IP source guard (see "Configuring Static Bindings for IP Source Guard" on page 315).

### WEB INTERFACE

To set the IP Source Guard filter for ports:

1. Click Security, IP Source Guard, Port Configuration.
2. Set the required filtering type for each port.
3. Click Apply

**Figure 61: Setting the Filter Type for IP Source Guard**




## Configuring Static Bindings for IP Source Guard

Use the Security > IP Source Guard > Static Configuration page to bind a static address to a port. Table entries include a MAC address, IP address, lease time, entry type (Static, Dynamic), VLAN identifier, and port identifier. All static entries are configured with an infinite lease time, which is indicated with a value of zero in the table.

### CLI REFERENCES

■ "ip source-guard binding" on page 769

### COMMAND USAGE

■ Static addresses entered in the source guard binding table are automatically configured with an infinite lease time. Dynamic entries learned via DHCP snooping are configured by the DHCP server itself.

■ Static bindings are processed as follows:

- ◆ If there is no entry with the same VLAN ID and MAC address, a new entry is added to the binding table using the type "static IP source guard binding."
- ◆ If there is an entry with the same VLAN ID and MAC address, and the type of entry is static IP source guard binding, then the new entry will replace the old one.

- If there is an entry with the same VLAN ID and MAC address, and the type of the entry is dynamic DHCP snooping binding, then the new entry will replace the old one and the entry type will be changed to static IP source guard binding.
- Only unicast addresses are accepted for static bindings.

## PARAMETERS

These parameters are displayed in the web interface:

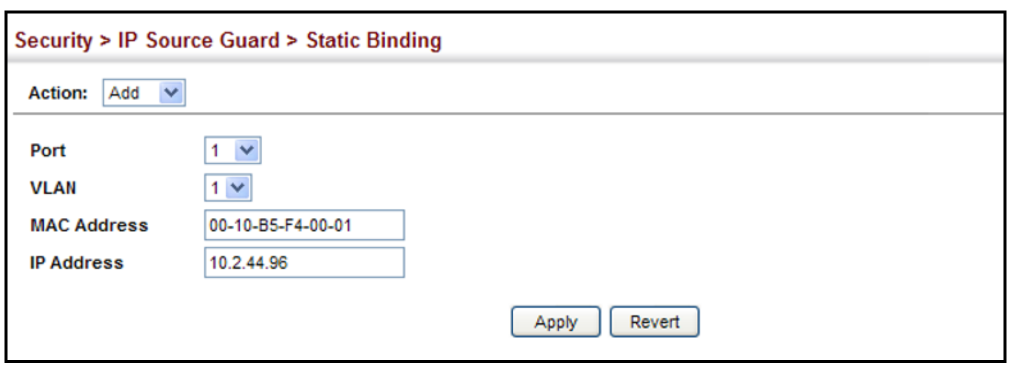
- **Port** – The port to which a static entry is bound.
- **VLAN** – ID of a configured VLAN (Range: 1-4093)
- **MAC Address** – A valid unicast MAC address.
- **IP Address** – A valid unicast IP address, including classful types A, B or C.

## WEB INTERFACE

To configure static bindings for IP Source Guard:

1. Click Security, IP Source Guard, Static Configuration.
2. Select Add from the Action list.
3. Enter the required bindings for each port.
4. Click Apply

**Figure 62: Configuring Static Bindings for IP Source Guard**

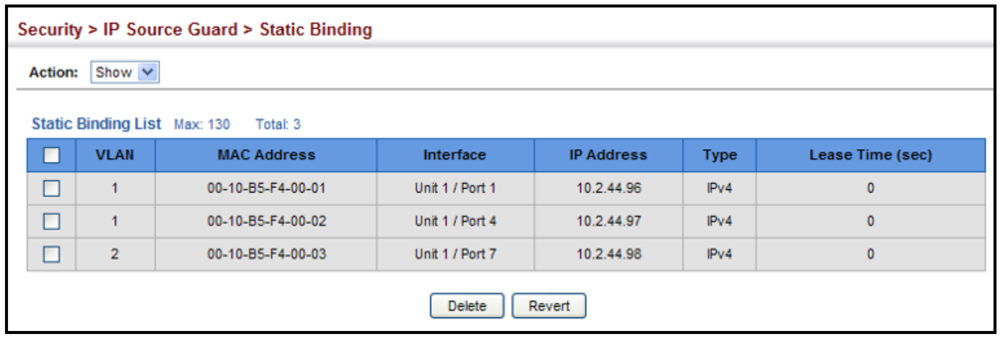


To display static bindings for IP Source Guard:

1. Click Security, IP Source Guard, Static Configuration.

2. Select Show from the Action list.

**Figure 63: Displaying Static Bindings for IP Source Guard**




## Displaying Information for Dynamic IP Source Guard Bindings

Use the Security > IP Source Guard > Dynamic Binding page to display the source-guard binding table for a selected interface.

### CLI References

- "show ip dhcp snooping binding" on page 768

### Parameters

These parameters are displayed in the web interface:

*Query by*

- **Port** – A port on this switch.
- **VLAN** – ID of a configured VLAN (Range: 1-4093)
- **MAC Address** – A valid unicast MAC address.
- **IP Address** – A valid unicast IP address, including classful types A, B or C.

*Dynamic Binding List*

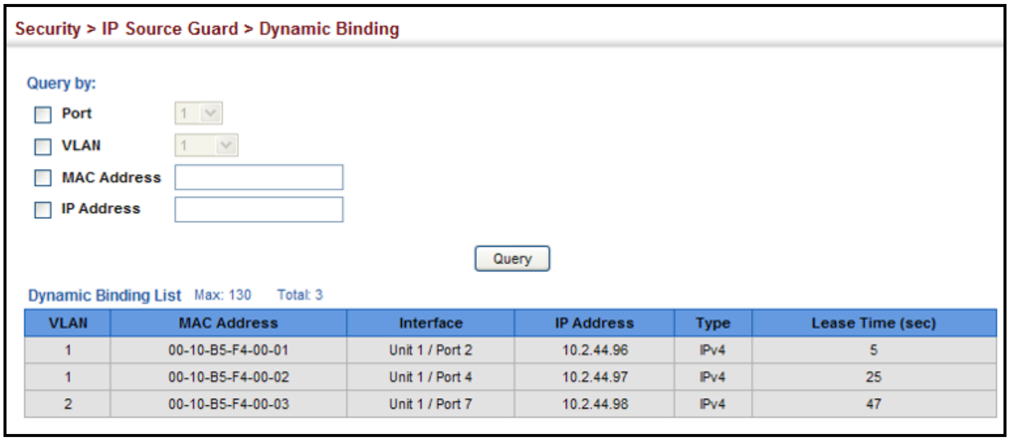
- **VLAN** – VLAN to which this entry is bound.
- **MAC Address** – Physical address associated with the entry.
- **Interface** – Port to which this entry is bound.
- **IP Address** – IP address corresponding to the client.
- **Type** – Static or dynamic binding.
- **Lease Time** – The time for which this IP address is leased to the client.

### WEB INTERFACE

To display the binding table for IP Source Guard:

1. Click Security, IP Source Guard, Dynamic Binding.
2. Mark the search criteria, and enter the required values.
3. Click Query

**Figure 64: Showing the IP Source Guard Binding Table**




## DHCP SNOOPING

The addresses assigned to DHCP clients on insecure ports can be carefully controlled using the dynamic bindings registered with DHCP Snooping (or using the static bindings configured with IP Source Guard). DHCP snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port.

### COMMAND USAGE

*DHCP Snooping Process*

- Network traffic may be disrupted when malicious DHCP messages are received from an outside source. DHCP snooping is used to filter DHCP messages received on a non-secure interface from outside the network or fire wall. When DHCP snooping is enabled globally and enabled on a VLAN interface, DHCP messages received on an untrusted interface from a device not listed in the DHCP snooping table will be dropped.
- Table entries are only learned for trusted interfaces. An entry is added or removed dynamically to the DHCP snooping table when a client receives or releases an IP address from a DHCP server. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier.

- The rate limit for the number of DHCP messages that can be processed by the switch is 100 packets per second. Any DHCP packets in excess of this limit are dropped.

- When DHCP snooping is enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.

- Filtering rules are implemented as follows:

  - If the global DHCP snooping is disabled, all DHCP packets are forwarded.

  - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a *trusted* port. If the received packet is a DHCP ACK message, a dynamic DHCP snooping entry is also added to the binding table.

  - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is *not trusted*, it is processed as follows:

    - If the DHCP packet is a reply packet from a DHCP server (including OFFER, ACK or NAK messages), the packet is dropped.

    - If the DHCP packet is from a client, such as a DECLINE or RELEASE message, the switch forwards the packet only if the corresponding entry is found in the binding table.

    - If the DHCP packet is from a client, such as a DISCOVER, REQUEST, INFORM, DECLINE or RELEASE message, the packet is forwarded if MAC address verification is disabled. However, if MAC address verification is enabled, then the packet will only be forwarded if the client's hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.

    - If the DHCP packet is not a recognizable type, it is dropped.

  - If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.

  - If a DHCP packet is from server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.

  - If the DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.

  - *Additional considerations when the switch itself is a DHCP client* – The port(s) through which the switch submits a client request to the DHCP server must be configured as trusted. Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCP server. Also, when the switch sends out DHCP client packets for itself, no filtering takes place. However, when the switch receives any messages from a DHCP server, any packets received from untrusted ports are dropped.

*DHCP Snooping Option 82*

- DHCP provides a relay mechanism for sending information about its DHCP clients or the relay agent itself to the DHCP server. Also known as DHCP Option 82, it allows compatible DHCP servers to use the information when assigning IP addresses, or to set other services or policies for clients. It is also an effective tool in preventing malicious network attacks from attached clients on DHCP services, such as IP Spoofing, Client Identifier Spoofing, MAC Address Spoofing, and Address Exhaustion.

- DHCP Snooping must be enabled for Option 82 information to be inserted into request packets.

- When the DHCP Snooping Information Option 82 is enabled, the requesting client (or an intermediate relay agent that has used the information fields to describe itself) can be identified in the DHCP request packets forwarded by the switch and in reply packets sent back from the DHCP server. This information may specify the MAC address or IP address of the requesting device (that is, the switch in this context).

  By default, the switch also fills in the Option 82 circuit-id field with information indicating the local interface over which the switch received the DHCP client request, including the port and VLAN ID. This allows DHCP client-server exchange messages to be forwarded between the server and client without having to flood them to the entire VLAN.

- If DHCP Snooping Information Option 82 is enabled on the switch, information may be inserted into a DHCP request packet received over any VLAN (depending on DHCP snooping filtering rules). The information inserted into the relayed packets includes the circuit-id and remote-id, as well as the gateway Internet address.

- When the switch receives DHCP packets from clients that already include DHCP Option 82 information, the switch can be configured to set the action policy for these packets. The switch can either drop the DHCP packets, keep the existing information, or replace it with the switch's relay information.

## DHCP Snooping Configuration

Use the IP Service > DHCP > Snooping (Configure Global) page to enable DHCP Snooping globally on the switch, or to configure MAC Address Verification.

### CLI REFERENCES

- "DHCP Snooping" on page 761

### PARAMETERS

These parameters are displayed in the web interface:

- **DHCP Snooping Status –** Enables DHCP snooping globally. (Default: Disabled)

- **DHCP Snooping MAC-Address Verification** – Enables or disables MAC address verification. If the source MAC address in the Ethernet header of the packet is not same as the client's hardware address in the DHCP packet, the packet is dropped. (Default: Enabled)

- **DHCP Snooping Information Option Status** – Enables or disables DHCP Option 82 information relay. (Default: Disabled)

■ **DHCP Snooping Information Option Policy** – Specifies how to handle DHCP client request packets which already contain Option 82 information.

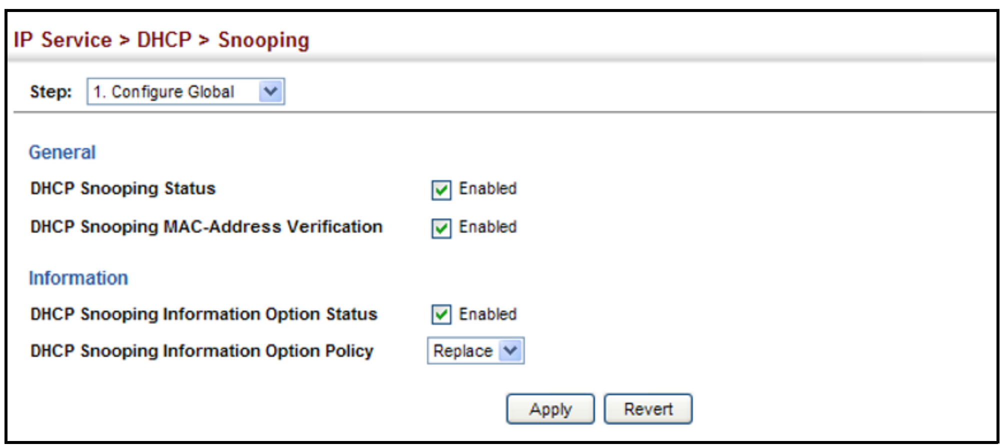
- **Drop** – Drops the client's request packet instead of relaying it.
- **Keep** – Retains the Option 82 information in the client request, and forwards the packets to trusted ports.
- **Replace** – Replaces the Option 82 information circuit-id and remote-id fields in the client's request with information about the relay agent itself, inserts the relay agent's address (when DHCP snooping is enabled), and forwards the packets to trusted ports. (This is the default policy.)

### WEB INTERFACE

To configure global settings for DHCP Snooping:

1. Click Security, IP Source Guard, DHCP Snooping.
2. Select Configure Global from the Step list.
3. Select the required options for the general DHCP snooping process and for the DHCP Option 82 information policy.
4. Click Apply

**Figure 65: Configuring Global Settings for DHCP Snooping**




## DHCP Snooping VLAN Configuration

Use the IP Service > DHCP > Snooping (Configure VLAN) page to enable or disable DHCP snooping on specific VLANs.

### CLI REFERENCES

■ "ip dhcp snooping vlan" on page 765

### COMMAND USAGE

■ When DHCP snooping is enabled globally on the switch, and enabled on the specified VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN.

- When the DHCP snooping is globally disabled, DHCP snooping can still be configured for specific VLANs, but the changes will not take effect until DHCP snooping is globally re-enabled.

- When DHCP snooping is globally enabled, and DHCP snooping is then disabled on a VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.

### PARAMETERS
These parameters are displayed in the web interface:

- **VLAN** – ID of a configured VLAN. (Range: 1-4093)

- **DHCP Snooping Status** – Enables or disables DHCP snooping for the selected VLAN. When DHCP snooping is enabled globally on the switch, and enabled on the specified VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN. (Default: Disabled)

### WEB INTERFACE
To configure global settings for DHCP Snooping:

1. Click Security, IP Source Guard, DHCP Snooping.

2. Select Configure VLAN from the Step list.

3. Enable DHCP Snooping on any existing VLAN.

4. Click Apply

**Figure 66: Configuring DHCP Snooping on a VLAN**


## Configuring Ports for DHCP Snooping

Use the IP Service > DHCP > Snooping (Configure Interface) page to configure switch ports as trusted or untrusted.

### CLI REFERENCES
- "ip dhcp snooping trust" on page 766

### COMMAND USAGE
- A trusted interface is an interface that is configured to receive only messages from within the network. An untrusted interface is an interface that is configured to receive messages from outside the network or fire wall.

- When DHCP snooping is enabled both globally and on a VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN.
- When an untrusted port is changed to a trusted port, all the dynamic DHCP snooping bindings associated with this port are removed.
- Set all ports connected to DHCP servers within the local network or fire wall to trusted state. Set all other ports outside the local network or fire wall to untrusted state.

### PARAMETERS

These parameters are displayed in the web interface:

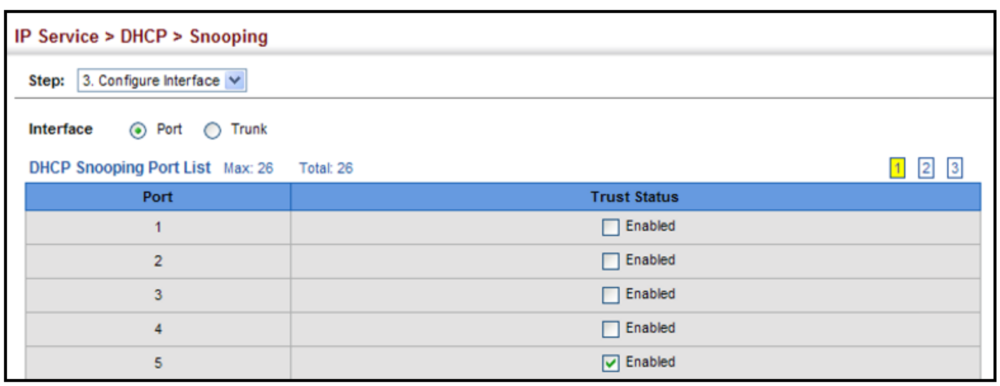
- **Trust Status** – Enables or disables a port as trusted. (Default: Disabled)

### WEB INTERFACE

To configure global settings for DHCP Snooping:

1. Click Security, IP Source Guard, DHCP Snooping.
2. Select Configure Interface from the Step list.
3. Set any ports within the local network or firewall to trusted.
4. Click Apply

**Figure 67: Configuring the Port Mode for DHCP Snooping**




## Displaying DHCP Snooping Binding Information

Use the IP Service > DHCP > Snooping (Show Information) page to display entries in the binding table.

### CLI REFERENCES

- "show ip dhcp snooping binding" on page 768

### PARAMETERS

These parameters are displayed in the web interface:

- **MAC Address** – Physical address associated with the entry.

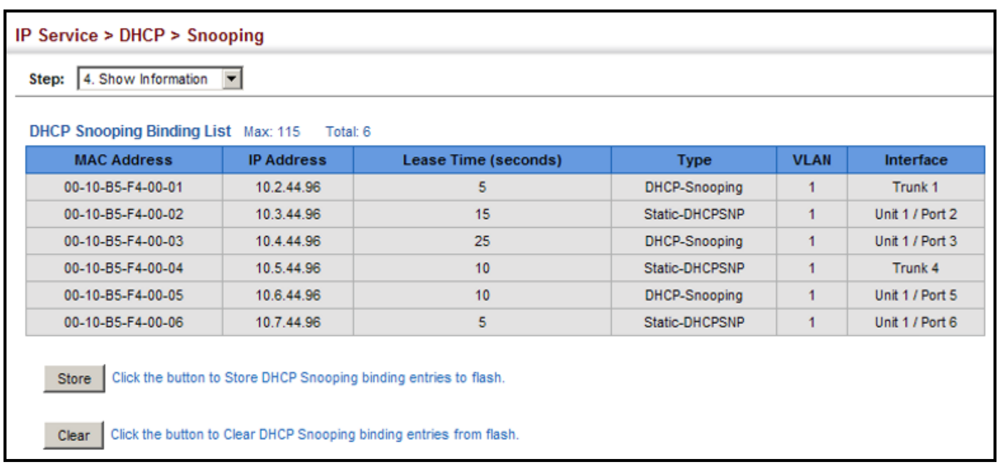
- **IP Address** – IP address corresponding to the client.
- **Lease Time** (seconds) – The time for which this IP address is leased to the client.
- **Type** – Entry types include:
  - **DHCP-Snooping** – Dynamically snooped.
  - **Static-DHCPSNP** – Statically configured.
- **VLAN** – VLAN to which this entry is bound.
- **Interface** – Port or trunk to which this entry is bound.
- **Store** – Writes all dynamically learned snooping entries to flash memory. This function can be used to store the currently learned dynamic DHCP snooping entries to flash memory. These entries will be restored to the snooping table when the switch is reset. However, note that the lease time shown for a dynamic entry that has been restored from flash memory will no longer be valid.
- **Clear** – Removes all dynamically learned snooping entries from flash memory.

### WEB INTERFACE

To display the binding table for DHCP Snooping:

1. Click Security, IP Source Guard, DHCP Snooping.
2. Select Show Information from the Step list.
3. Use the Store or Clear function if required.

**Figure 68: Displaying the Binding Table for DHCP Snooping**




| MAC Address | IP Address | Lease Time (seconds) | Type | VLAN | Interface |
|---|---|---|---|---|---|
| 00-10-B5-F4-00-01 | 10.2.44.96 | 5 | DHCP-Snooping | 1 | Trunk 1 |
| 00-10-B5-F4-00-02 | 10.3.44.96 | 15 | Static-DHCPSNP | 1 | Unit 1 / Port 2 |
| 00-10-B5-F4-00-03 | 10.4.44.96 | 25 | DHCP-Snooping | 1 | Unit 1 / Port 3 |
| 00-10-B5-F4-00-04 | 10.5.44.96 | 10 | Static-DHCPSNP | 1 | Trunk 4 |
| 00-10-B5-F4-00-05 | 10.6.44.96 | 10 | DHCP-Snooping | 1 | Unit 1 / Port 5 |
| 00-10-B5-F4-00-06 | 10.7.44.96 | 5 | Static-DHCPSNP | 1 | Unit 1 / Port 6 |

# 15 BASIC ADMINISTRATION PROTOCOLS

This chapter describes basic administration tasks including:

- Event Logging – Sets conditions for logging event messages to system memory or flash memory, configures conditions for sending trap messages to remote log servers, and configures trap reporting to remote hosts using Simple Mail Transfer Protocol (SMTP).
- Link Layer Discovery Protocol (LLDP) – Configures advertisement of basic information about the local switch, or discovery of information about neighboring devices on the local broadcast domain.
- Simple Network Management Protocol (SNMP) – Configures switch management through SNMPv1, SNMPv2c or SNMPv3.
- Remote Monitoring (RMON) – Configures local collection of detailed statistics or events which can be subsequently retrieved through SNMP.

## CONFIGURING EVENT LOGGING

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

### System Log Configuration

Use the Administration > Log > System (Configure Global) page to enable or disable event logging, and specify which levels are logged to RAM or flash memory.

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

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

**CLI REFERENCES**

- "Event Logging" on page 640

### Parameters

These parameters are displayed in the web interface:

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

- **Flash Level** – Limits log messages saved to the switch's permanent flash memory for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be logged to flash. (Range: 0-7, Default: 3)

**Table 1: Logging Levels**

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

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

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

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

### Web Interface

To configure the logging of error messages to system memory:

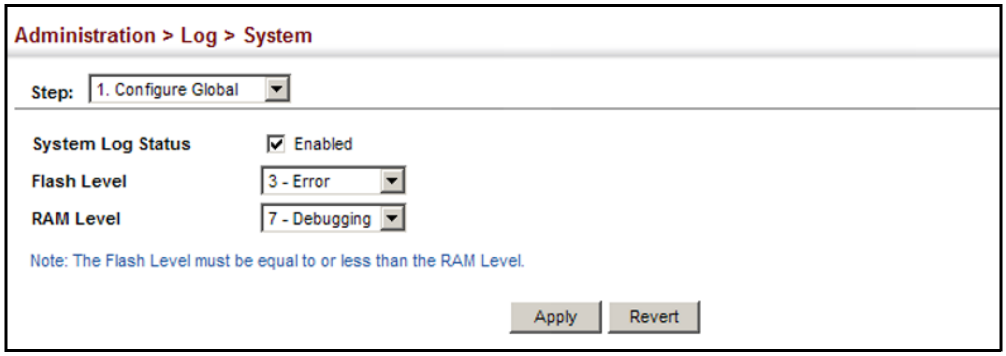
1. Click Administration, Log, System.

2. Select Configure Global from the Step list.

3. Enable or disable system logging, set the level of event messages to be logged to flash memory and RAM.

4. Click Apply.

**Figure 1: Configuring Settings for System Memory Logs**

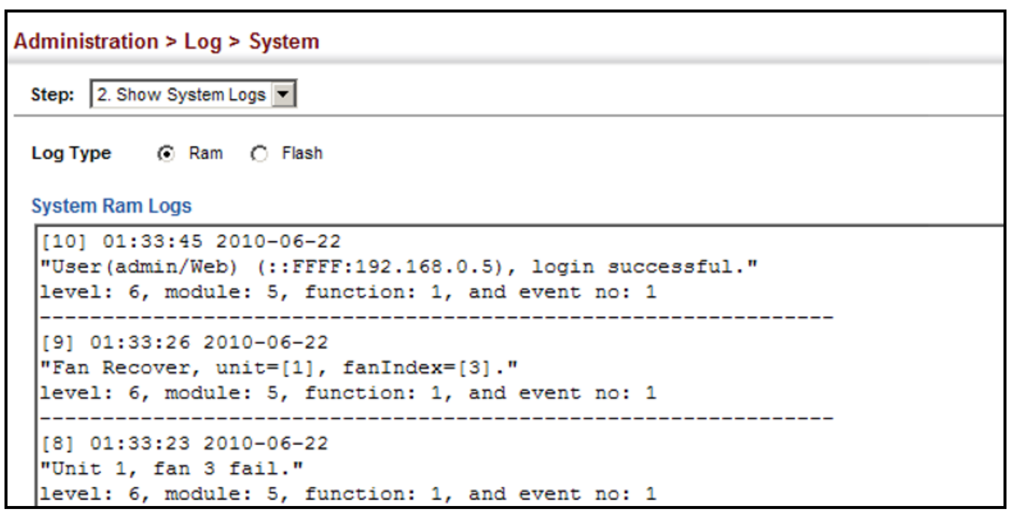



To show the error messages logged to system memory:

1. Click Administration, Log, System.
2. Select Show System Logs from the Step list.
3. Click RAM or Flash.

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

**Figure 2: Showing Error Messages Logged to System Memory**



## Remote Log Configuration

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

### CLI References

■"Event Logging" on page 640

### Parameters

These parameters are displayed in the web interface:

- **Remote Log Status** – Enables/disables the logging of debug or error messages to the remote logging process. (Default: Disabled)
- **Logging Facility** – Sets the facility type for remote logging of syslog messages. There are eight facility types specified by values of 16 to 23. The facility type is used by the syslog server to dispatch log messages to an appropriate service.

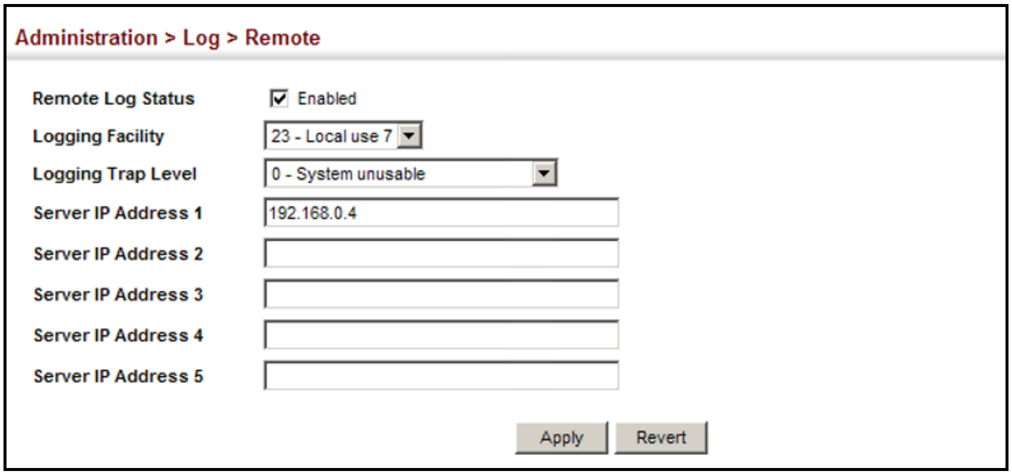
  The attribute specifies the facility type tag sent in syslog messages (see RFC 3164). This type has no effect on the kind of messages reported by the switch. However, it may be used by the syslog server to process messages, such as sorting or storing messages in the corresponding database. (Range: 16-23, Default: 23)
- **Logging Trap Level** – Limits log messages that are sent to the remote syslog server for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be sent to the remote server. (Range: 0-7, Default: 7)
- **Server IP Address** – Specifies the IPv4 or IPv6 address of a remote server which will be sent syslog messages.

### Web Interface

To configure the logging of error messages to remote servers:

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

**Figure 3: Configuring Settings for Remote Logging of Error Messages**




## Sending Simple Mail Transfer Protocol Alerts

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

### CLI References

- "SMTP Alerts" on page 646

### Parameters

These parameters are displayed in the web interface:

- **SMTP Status** – Enables/disables the SMTP function. (Default: Enabled)
- **Severity** – Sets the syslog severity threshold level (see table on page 326) used to trigger alert messages. All events at this level or higher will be sent to the configured email recipients. For example, using Level 7 will report all events from level 7 to level 0. (Default: Level 7)
- **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.
- **Email Destination Address** – Specifies the email recipients of alert messages. You can specify up to five recipients.
- **Server IP Address** – Specifies a list of up to three recipient SMTP servers. The switch attempts to connect to the other listed servers if the first fails.

### Web Interface

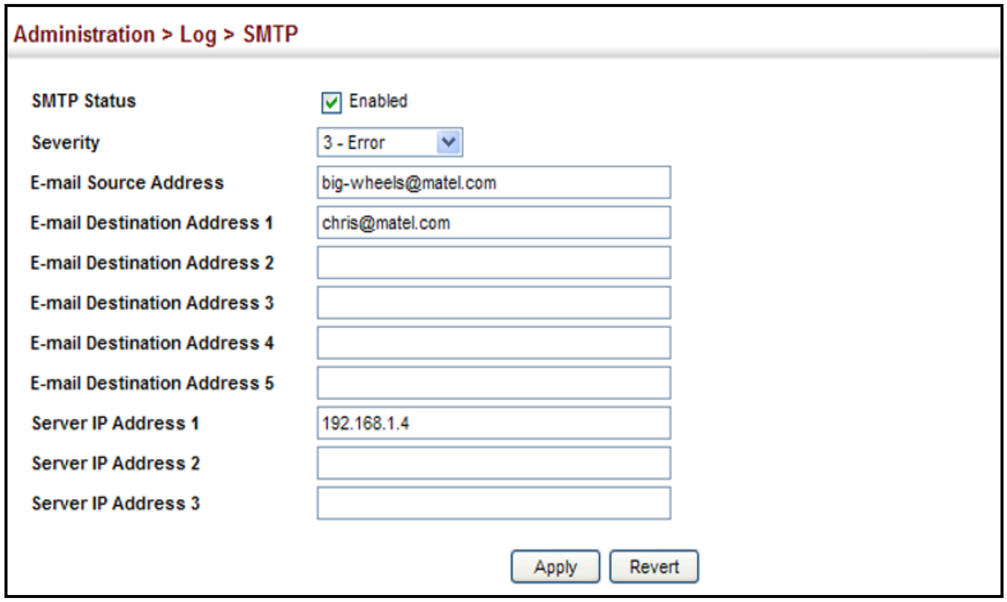
To configure SMTP alert messages:

1. Click Administration, Log, SMTP.

2. Enable SMTP, specify a source email address, and select the minimum severity level. Specify the source and destination email addresses, and one or more SMTP servers.

3. Click Apply.

**Figure 4: Configuring SMTP Alert Messages**




## Link Layer Discovery Protocol

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

### Setting LLDP Timing Attributes

Use the Administration > LLDP (Configure Global) page to set attributes for general functions such as globally enabling LLDP on the switch, setting the message ageout time, and setting the frequency for broadcasting general advertisements or reports about changes in the LLDP MIB.

#### CLI References

■ "LLDP Commands" on page 1013

#### Parameters

These parameters are displayed in the web interface:

■ **LLDP** – Enables LLDP globally on the switch. (Default: Enabled)

- **Transmission Interval** – Configures the periodic transmit interval for LLDP advertisements. (Range: 5-32768 seconds; Default: 30 seconds)

  This attribute must comply with the following rule:
  (Transmission Interval * Hold Time Multiplier) ≤ 65536, and
  Transmission Interval >= (4 * Delay Interval)

- **Hold Time Multiplier** – Configures the time-to-live (TTL) value sent in LLDP advertisements as shown in the formula below. (Range: 2-10; Default: 4)

  The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner.

  TTL in seconds is based on the following rule:
  (Transmission Interval * Holdtime Multiplier) ≤ 65536.

  Therefore, the default TTL is 4*30 = 120 seconds.

- **Delay Interval** – Configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables. (Range: 1-8192 seconds; Default: 2 seconds)

  The transmit delay is used to prevent a series of successive LLDP transmissions during a short period of rapid changes in local LLDP MIB objects, and to increase the probability that multiple, rather than single changes, are reported in each transmission.

  This attribute must comply with the rule:
  (4 * Delay Interval) ≤ Transmission Interval

- **Reinitialization Delay** – Configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down. (Range: 1-10 seconds; Default: 2 seconds)

  When LLDP is re-initialized on a port, all information in the remote systems LLDP MIB associated with this port is deleted.

- **Notification Interval** – Configures the allowed interval for sending SNMP notifications about LLDP MIB changes. (Range: 5-3600 seconds; Default: 5 seconds)

  This parameter only applies to SNMP applications which use data stored in the LLDP MIB for network monitoring or management.

  Information about changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

### WEB INTERFACE

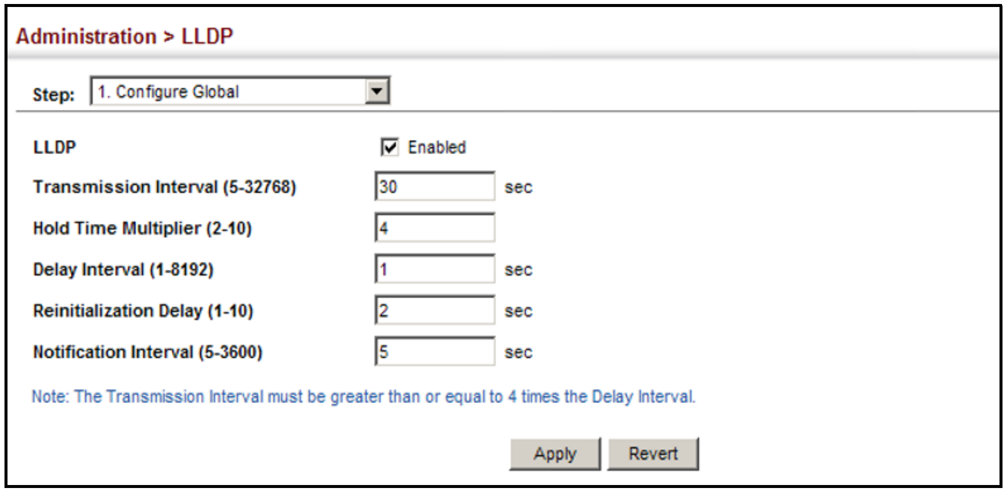
To configure LLDP timing attributes:

1. Click Administration, LLDP.
2. Select Configure Global from the Step list.

**3.** Enable LLDP, and modify any of the timing parameters as required.

**4.** Click Apply.

**Figure 5: Configuring LLDP Timing Attributes**




## Configuring LLDP Interface Attributes

Use the Administration > LLDP (Configure Interface) page to specify the message attributes for individual interfaces, including whether messages are transmitted, received, or both transmitted and received, whether SNMP notifications are sent, and the type of information advertised.

### CLI REFERENCES

■ "LLDP Commands" on page 1013

### PARAMETERS

These parameters are displayed in the web interface:

■ **Admin Status** – Enables LLDP message transmit and receive modes for LLDP Protocol Data Units. (Options: Tx only, Rx only, TxRx, Disabled; Default: TxRx)

■ **SNMP Notification** – Enables the transmission of SNMP trap notifications about LLDP and LLDP-MED changes. (Default: Enabled)

This option sends out SNMP trap notifications to designated target stations at the interval specified by the Notification Interval in the preceding section. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), the LLDP-MED MIB (ANSI/TIA-1057), or vendor-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs.

For information on defining SNMP trap destinations, see "Specifying Trap Managers" on page 360.

Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

- **Basic Optional TLVs** – Configures basic information included in the TLV field of advertised messages.
  - **Management Address** – The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.

    The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address. The interface number and OID are included to assist SNMP applications in the performance of network discovery by indicating enterprise specific or other starting points for the search, such as the Interface or Entity MIB.

    Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV.

    Every management address TLV that reports an address that is accessible on a port and protocol VLAN through the particular port should be accompanied by a port and protocol VLAN TLV that indicates the VLAN identifier (VID) associated with the management address reported by this TLV.
  - **Port Description** – The port description is taken from the ifDescr object in RFC 2863, which includes information about the manufacturer, the product name, and the version of the interface hardware/software.
  - **System Capabilities** – The system capabilities identifies the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.
  - **System Description** – The system description is taken from the sysDescr object in RFC 3418, which includes the full name and version identification of the system's hardware type, software operating system, and networking software.
  - **System Name** – The system name is taken from the sysName object in RFC 3418, which contains the system's administratively assigned name. To configure the system name, see "Displaying System Information" on page 85.
- **802.1 Organizationally Specific TLVs** – Configures IEEE 802.1 information included in the TLV field of advertised messages.
  - **Protocol Identity** – The protocols that are accessible through this interface (see "Protocol VLANs" on page 161).
  - **VLAN ID** – The port's default VLAN identifier (PVID) indicates the VLAN with which untagged or priority-tagged frames are associated (see "IEEE 802.1Q VLANs" on page 137).
  - **VLAN Name** – The name of all VLANs to which this interface has been assigned (see "IEEE 802.1Q VLANs" on page 137 and "Protocol VLANs" on page 161).

- **Port And Protocol VLAN ID** – The port-based and protocol-based VLANs configured on this interface (the port-based and protocol-based VLANs configured on this interface (see "IEEE 802.1Q VLANs" on page 137 and "Protocol VLANs" on page 161).

■ **802.3 Organizationally Specific TLVs** – Configures IEEE 802.3 information included in the TLV field of advertised messages.

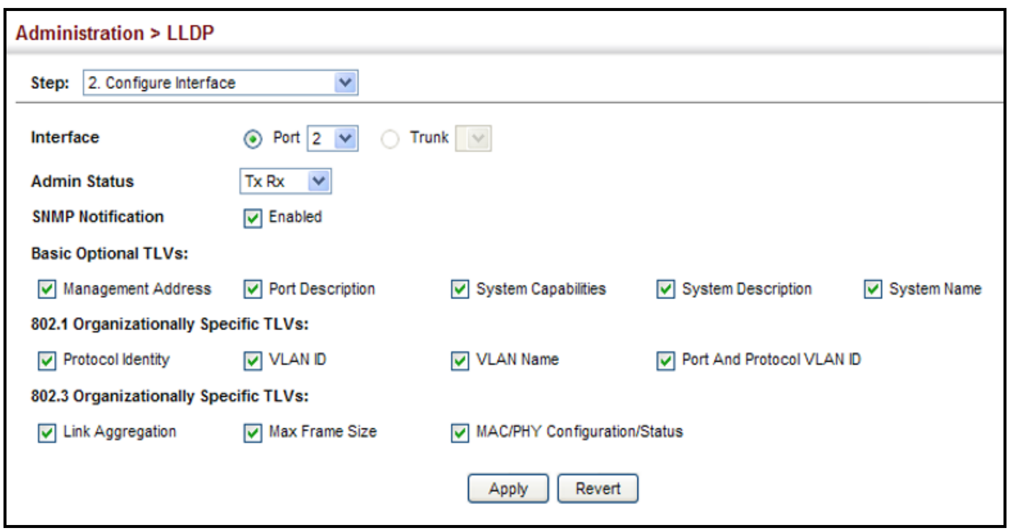
- **Link Aggregation** – The link aggregation capabilities, aggregation status of the link, and the IEEE 802.3 aggregated port identifier if this interface is currently a link aggregation member.
- **Max Frame Size** – The maximum frame size. (See "Configuring Support for Jumbo Frames" on page 88 for information on configuring the maximum frame size for this switch
- **MAC/PHY Configuration/Status** – The MAC/PHY configuration and status which includes information about auto-negotiation support/capabilities, and operational Multistation Access Unit (MAU) type.

### WEB INTERFACE

To configure LLDP interface attributes:

1. Click Administration, LLDP.
2. Select Configure Interface from the Step list.
3. Set the LLDP transmit/receive mode, specify whether or not to send SNMP trap messages, and select the information to advertise in LLDP messages.
4. Click Apply.

**Figure 6: Configuring LLDP Interface Attributes**



## Displaying LLDP Local Device Information

Use the Administration > LLDP (Show Local Device Information) page to display information about the switch, such as its MAC address, chassis ID, management IP address, and port information.

### CLI REFERENCES

- "show lldp info local-device" on page 1026

### PARAMETERS

These parameters are displayed in the web interface:

*Global Settings*

- **Chassis Type** – Identifies the chassis containing the IEEE 802 LAN entity associated with the transmitting LLDP agent. There are several ways in which a chassis may be identified and a chassis ID subtype is used to indicate the type of component being referenced by the chassis ID field.

**Table 2: Chassis ID Subtype**

| ID Basis | Reference |
|---|---|
| Chassis component | EntPhysicalAlias when entPhysClass has a value of ‘chassis(3)’ (IETF RFC 2737) |
| Interface alias | IfAlias (IETF RFC 2863) |
| Port component | EntPhysicalAlias when entPhysicalClass has a value ‘port(10)’ or ‘backplane(4)’ (IETF RFC 2737) |
| MAC address | MAC address (IEEE Std 802-2001) |
| Network address | networkAddress |
| Interface name | ifName (IETF RFC 2863) |
| Locally assigned | locally assigned |

- **Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.
- **System Name** – A string that indicates the system’s administratively assigned name (see "Displaying System Information" on page 85).
- **System Description** – A textual description of the network entity. This field is also displayed by the **show system** command.
- **System Capabilities Supported** – The capabilities that define the primary function(s) of the system.

**Table 3: System Capabilities**

| ID Basis | Reference |
|---|---|
| Other | — |
| Repeater | IETF RFC 2108 |
| Bridge | IETF RFC 2674 |
| WLAN Access Point | IEEE 802.11 MIB |

**Table 3: System Capabilities (Continued)**

| ID Basis | Reference |
|---|---|
| Router | IETF RFC 1812 |
| Telephone | IETF RFC 2011 |
| DOCSIS cable device | IETF RFC 2669 and IETF RFC 2670 |
| End Station Only | IETF RFC 2011 |

- **System Capabilities Enabled** – The primary function(s) of the system which are currently enabled. Refer to the preceding table.

- **Management Address** – The management address associated with the local system.

*Interface Settings*

The attributes listed below apply to both port and trunk interface types. When a trunk is listed, the descriptions apply to the first port of the trunk.

- **Port/Trunk Description** – A string that indicates the port or trunk description. If RFC 2863 is implemented, the ifDescr object should be used for this field.

- **Port/Trunk ID** – A string that contains the specific identifier for the port or trunk from which this LLDPDU was transmitted.

### WEB INTERFACE

To display LLDP information for the local device:

1. Click Administration, LLDP.
2. Select Show Local Device Information from the Step list.
3. Select General, Port, or Trunk.

**Figure 7: Displaying Local Device Information for LLDP** (General)

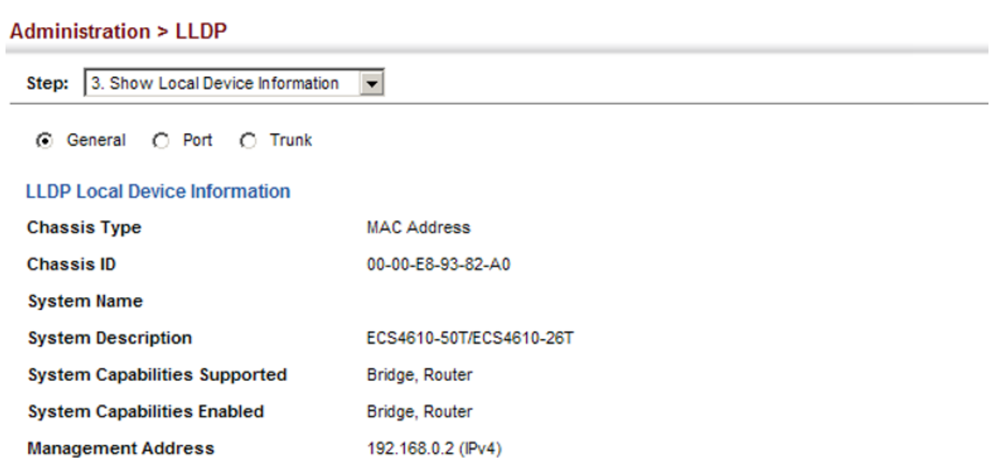
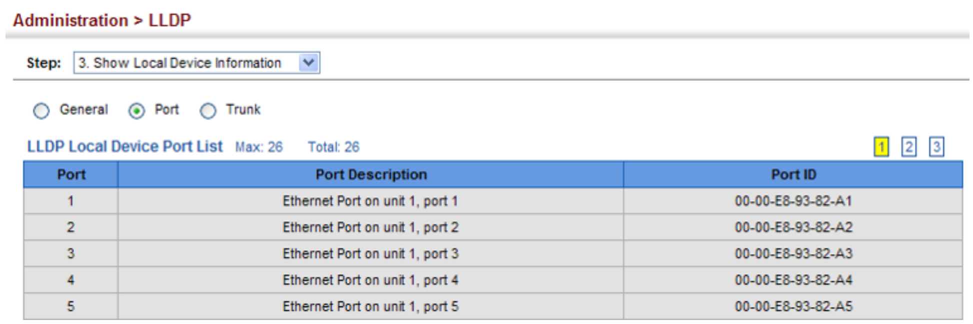


**Figure 8: Displaying Local Device Information for LLDP** (Port)




| Port | Port Description | Port ID |
|---|---|---|
| 1 | Ethernet Port on unit 1, port 1 | 00-00-E8-93-82-A1 |
| 2 | Ethernet Port on unit 1, port 2 | 00-00-E8-93-82-A2 |
| 3 | Ethernet Port on unit 1, port 3 | 00-00-E8-93-82-A3 |
| 4 | Ethernet Port on unit 1, port 4 | 00-00-E8-93-82-A4 |
| 5 | Ethernet Port on unit 1, port 5 | 00-00-E8-93-82-A5 |

## Displaying LLDP Remote Port Information

Use the Administration > LLDP (Show Remote Device Information) page to display information about devices connected directly to the switch's ports which are advertising information through LLDP, or to display detailed information about an LLDP-enabled device connected to a specific port on the local switch.

### CLI REFERENCES

■"show lldp info remote-device" on page 1027

### PARAMETERS

These parameters are displayed in the web interface:

*Port*

■**Local Port** – The local port to which a remote LLDP-capable device is attached.

■**Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.

■**Port ID** – A string that contains the specific identifier for the port from which this LLDPDU was transmitted.

■**System Name** – A string that indicates the system's administratively assigned name.

*Port Details*

■**Local Port** – The local port to which a remote LLDP-capable device is attached.

■**Chassis Type** – Identifies the chassis containing the IEEE 802 LAN entity associated with the transmitting LLDP agent. There are several ways in which a chassis may be identified and a chassis ID subtype is used to indicate the type of component being referenced by the chassis ID field. (See Table 2, "Chassis ID Subtype," on page 335.)

■**Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.

■**System Name** – A string that indicates the system's assigned name.

- **System Description** – A textual description of the network entity.
- **Management Address** – The IPv4 address of the remote device. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.
- **Port Type** – Indicates the basis for the identifier that is listed in the Port ID field.

**Table 4: Port ID Subtype**

| ID Basis | Reference |
|---|---|
| Interface alias | IfAlias (IETF RFC 2863) |
| Chassis component | EntPhysicalAlias when entPhysClass has a value of 'chassis(3)' (IETF RFC 2737) |
| Port component | EntPhysicalAlias when entPhysicalClass has a value 'port(10)' or 'backplane(4)' (IETF RFC 2737) |
| MAC address | MAC address (IEEE Std 802-2001) |
| Network address | networkAddress |
| Interface name | ifName (IETF RFC 2863) |
| Agent circuit ID | agent circuit ID (IETF RFC 3046) |
| Locally assigned | locally assigned |

- **Port Description** – A string that indicates the port's description. If RFC 2863 is implemented, the ifDescr object should be used for this field.
- **Port ID** – A string that contains the specific identifier for the port from which this LLDPDU was transmitted.
- **System Capabilities Supported** – The capabilities that define the primary function(s) of the system. (See Table 3, "System Capabilities," on page 335.)
- **System Capabilities Enabled** – The primary function(s) of the system which are currently enabled. (See Table 3, "System Capabilities," on page 335.)
- **Management Address List** – The management addresses for this device. Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV.

*Port Details – 802.1 Extension Information*

- **Remote Port VID** – The port's default VLAN identifier (PVID) indicates the VLAN with which untagged or priority-tagged frames are associated.
- **Remote VLAN Name List** – VLAN names associated with a port.
- **Remote Protocol Identity List** – Information about particular protocols that are accessible through a port. This object represents an arbitrary local integer value used by this agent to identify a particular protocol identity, and an octet string used to identify the protocols associated with a port of the remote system.

*Port Details – 802.3 Extension Port Information*

- **Remote Port Auto-Neg Supported** – Shows whether the given port (associated with remote system) supports auto-negotiation.

- **Remote Port Auto-Neg Adv-Capability** – The value (bitmap) of the ifMauAutoNegCapAdvertisedBits object (defined in IETF RFC 3636) which is associated with a port on the remote system.

**Table 5: Remote Port Auto-Negotiation Advertised Capability**

| Bit | Capability |
|---|---|
| 0 | other or unknown |
| 1 | 10BASE-T half duplex mode |
| 2 | 10BASE-T full duplex mode |
| 3 | 100BASE-T4 |
| 4 | 100BASE-TX half duplex mode |
| 5 | 100BASE-TX full duplex mode |
| 6 | 100BASE-T2 half duplex mode |
| 7 | 100BASE-T2 full duplex mode |
| 8 | PAUSE for full-duplex links |
| 9 | Asymmetric PAUSE for full-duplex links |
| 10 | Symmetric PAUSE for full-duplex links |
| 11 | Asymmetric and Symmetric PAUSE for full-duplex links |
| 12 | 1000BASE-X, -LX, -SX, -CX half duplex mode |
| 13 | 1000BASE-X, -LX, -SX, -CX full duplex mode |
| 14 | 1000BASE-T half duplex mode |
| 15 | 1000BASE-T full duplex mode |

- **Remote Port Auto-Neg Status** – Shows whether port auto-negotiation is enabled on a port associated with the remote system.

- **Remote Port MAU Type** – An integer value that indicates the operational MAU type of the sending device. This object contains the integer value derived from the list position of the corresponding dot3MauType as listed in IETF RFC 3636 and is equal to the last number in the respective dot3MauType OID.

*Port Details – 802.3 Extension Power Information*

- **Remote Power Class** – The port Class of the given port associated with the remote system (PSE – Power Sourcing Equipment or PD – Powered Device).

- **Remote Power MDI Status** – Shows whether MDI power is enabled on the given port associated with the remote system.

- **Remote Power Pairs** – “Signal” means that the signal pairs only are in use, and “Spare” means that the spare pairs only are in use.

- **Remote Power MDI Supported** – Shows whether MDI power is supported on the given port associated with the remote system.

- **Remote Power Pair Controlable** – Indicates whether the pair selection can be controlled for sourcing power on the given port associated with the remote system.

- **Remote Power Classification** – This classification is used to tag different terminals on the Power over LAN network according to their power consumption. Devices such as IP telephones, WLAN access points and others, will be classified according to their power requirements.

*Port Details – 802.3 Extension Trunk Information*

- **Remote Link Aggregation Capable** – Shows if the remote port is not in link aggregation state and/or it does not support link aggregation.

- **Remote Link Aggregation Status** – The current aggregation status of the link.

- **Remote Link Aggregation Port ID** – This object contains the IEEE 802.3 aggregated port identifier, aAggPortID (IEEE 802.3-2002, 30.7.2.1.1), derived from the ifNumber of the ifIndex for the port component associated with the remote system. If the remote port is not in link aggregation state and/or it does not support link aggregation, this value should be zero.

*Port Details – 802.3 Extension Frame Information*

- **Remote Max Frame Size** – An integer value indicating the maximum supported frame size in octets on the port component associated with the remote system.

### Web Interface

To display LLDP information for a remote port:

1. Click Administration, LLDP.

2. Select Show Remote Device Information from the Step list.

3. Select Port, Port Details, Trunk, or Trunk Details.

**Figure 9: Displaying Remote Device Information for LLDP** (Port)

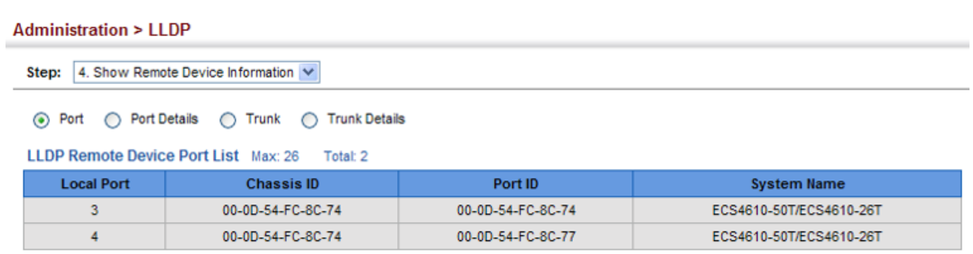
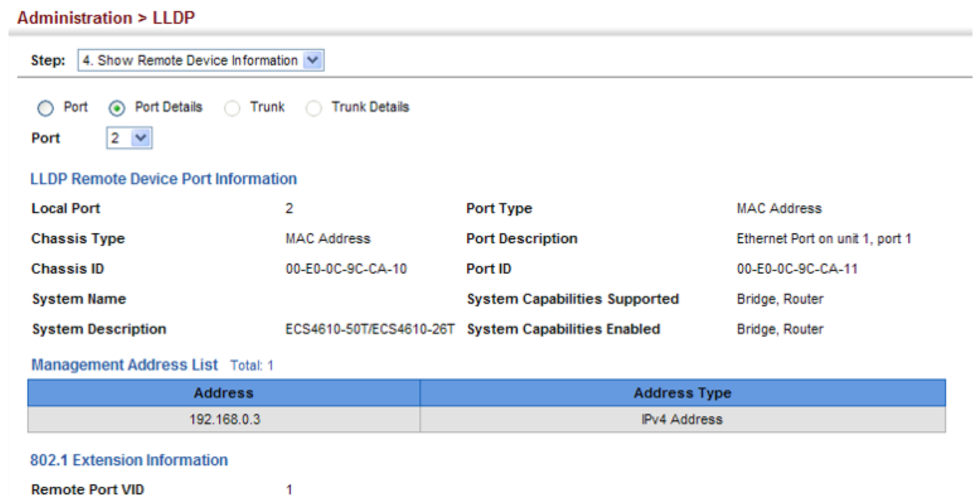


**Figure 10: Displaying Remote Device Information for LLDP** (Port Details)




## Displaying Device Statistics

Use the Administration > LLDP (Show Device Statistics) page to display statistics for LLDP-capable devices attached to the switch, and for LLDP protocol messages transmitted or received on all local interfaces.

### CLI REFERENCES

- "show lldp info statistics" on page 1028

### PARAMETERS

These parameters are displayed in the web interface:

*General Statistics on Remote Devices*

- **Neighbor Entries List Last Updated** – The time the LLDP neighbor entry list was last updated.
- **New Neighbor Entries Count** – The number of LLDP neighbors for which the remote TTL has not yet expired.
- **Neighbor Entries Deleted Count** – The number of LLDP neighbors which have been removed from the LLDP remote systems MIB for any reason.
- **Neighbor Entries Dropped Count** – The number of times which the remote database on this switch dropped an LLDPDU because of insufficient resources.
- **Neighbor Entries Age-out Count** – The number of times that a neighbor's information has been deleted from the LLDP remote systems MIB because the remote TTL timer has expired.

*Port/Trunk*

- **Frames Discarded** – Number of frames discarded because they did not conform to the general validation rules as well as any specific usage rules defined for the particular TLV.

- **Frames Invalid** – A count of all LLDPDUs received with one or more detectable errors.
- **Frames Received** – Number of LLDP PDUs received.
- **Frames Sent** – Number of LLDP PDUs transmitted.
- **TLVs Unrecognized** – A count of all TLVs not recognized by the receiving LLDP local agent.
- **TLVs Discarded** – A count of all LLDPDUs received and then discarded due to insufficient memory space, missing or out-of-sequence attributes, or any other reason.
- **Neighbor Ageouts** – A count of the times that a neighbor's information has been deleted from the LLDP remote systems MIB because the remote TTL timer has expired.

### WEB INTERFACE

To display statistics for LLDP-capable devices attached to the switch:

1. Click Administration, LLDP.
2. Select Show Device Statistics from the Step list.
3. Select General, Port, or Trunk.

**Figure 11: Displaying LLDP Device Statistics** (General)

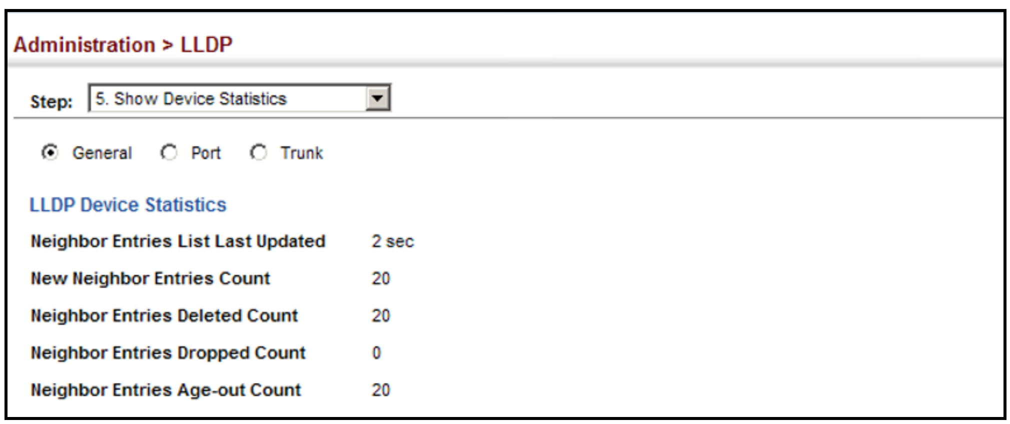
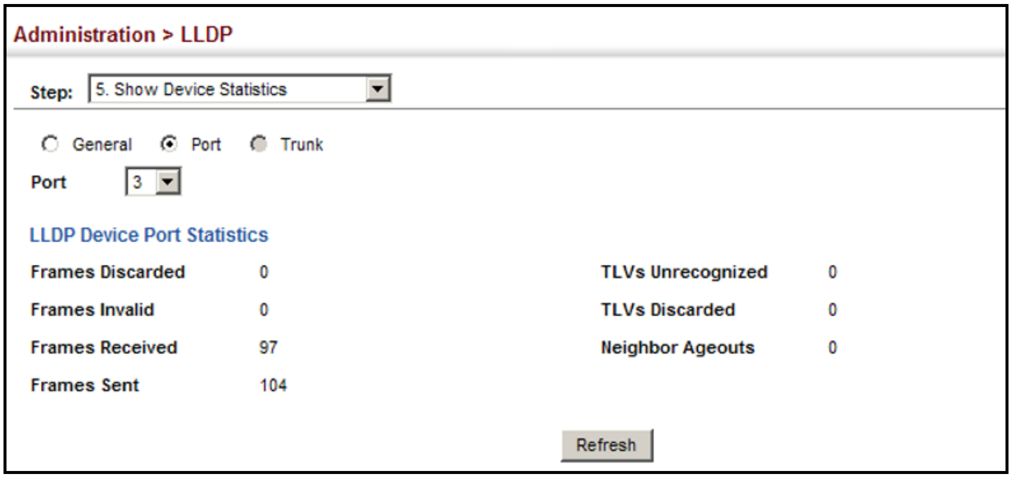


**Figure 12: Displaying LLDP Device Statistics** (Port)




## SIMPLE NETWORK MANAGEMENT PROTOCOL

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

Managed devices supporting SNMP contain software, which runs locally on the device and is referred to as an agent. A defined set of variables, known as managed objects, is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB) that provides a standard presentation of the information controlled by the agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

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

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

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

**Table 6: SNMPv3 Security Models and Levels**

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

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

### COMMAND USAGE

*Configuring SNMPv1/2c Management Access*

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

1. Use the Administration > SNMP (Configure Global) page to enable SNMP on the switch, and to enable trap messages.

2. Use the Administration > SNMP (Configure User - Add Community) page to configure the community strings authorized for management access.

3. Use the Administration > SNMP (Configure Trap) page to specify trap managers so that key events are reported by this switch to your management station.

*Configuring SNMPv3 Management Access*

1. Use the Administration > SNMP (Configure Global) page to enable SNMP on the switch, and to enable trap messages.

2. Use the Administration > SNMP (Configure Trap) page to specify trap managers so that key events are reported by this switch to your management station.

3. Use the Administration > SNMP (Configure Engine) page to change the local engine ID. If you want to change the default engine ID, it must be changed before configuring other parameters.

4. Use the Administration > SNMP (Configure View) page to specify read and write access views for the switch MIB tree.

5. Use the Administration > SNMP (Configure User) page to configure SNMP user groups with the required security model (i.e., SNMP v1, v2c or v3) and security level (i.e., authentication and privacy).

6. Use the Administration > SNMP (Configure Group) page to assign SNMP users to groups, along with their specific authentication and privacy passwords.

## Configuring Global Settings for SNMP

Use the Administration > SNMP (Configure Global) page to enable SNMPv3 service for all management clients (i.e., versions 1, 2c, 3), and to enable trap messages.

### CLI REFERENCES

- "snmp-server" on page 660
- "snmp-server enable traps" on page 663

### PARAMETERS

These parameters are displayed in the web interface:

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

- **Authentication Traps**[1] – Issues a notification message to specified IP trap managers whenever an invalid community string is submitted during the SNMP access authentication process. (Default: Enabled)

- **Link-up and Link-down Traps**[1] – Issues a notification message whenever a port link is established or broken. (Default: Enabled)

### WEB INTERFACE

To configure global settings for SNMP:

1. Click Administration, SNMP.

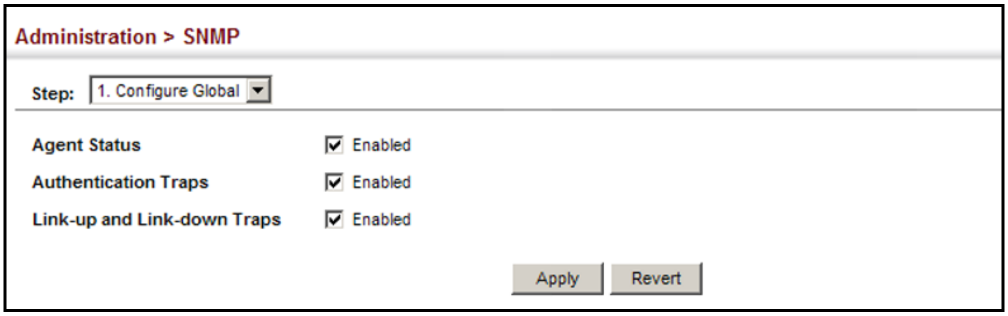
2. Select Configure Global from the Step list.

3. Enable SNMP and the required trap types.

4. Click Apply

1. These are legacy notifications and therefore when used for SNMPv3 hosts, they must be enabled in conjunction with the corresponding entries in the Notification View (page 348).

**Figure 13: Configuring Global Settings for SNMP**




## Setting the Local Engine ID

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

### CLI REFERENCES

- "snmp-server engine-id" on page 666

### COMMAND USAGE

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

### PARAMETERS

These parameters are displayed in the web interface:

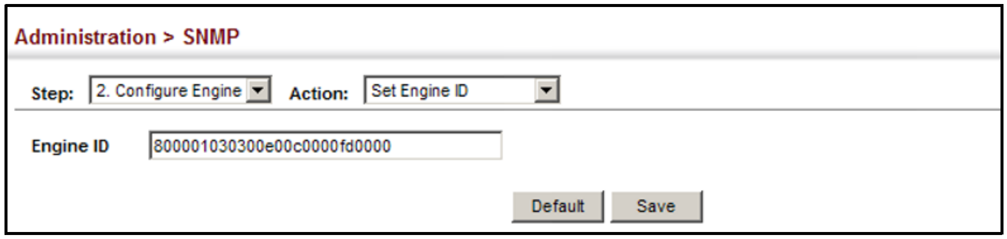
- **Engine ID** – A new engine ID can be specified by entering 9 to 64 hexadecimal characters (5 to 32 octets in hexadecimal format). If an odd number of characters are specified, a trailing zero is added to the value to fill in the last octet. For example, the value “123456789” is equivalent to “1234567890”.

### WEB INTERFACE

To configure the local SNMP engine ID:

1. Click Administration, SNMP.
2. Select Configure Engine from the Step list.
3. Select Set Engine ID from the Action list.
4. Enter an ID of a least 9 hexadecimal characters.
5. Click Apply

**Figure 14: Configuring the Local Engine ID for SNMP**




## Specifying a Remote Engine ID

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

### CLI References

- "snmp-server engine-id" on page 666

### Command Usage

- SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it. (See "Configuring Remote SNMPv3 Users" on page 358.)

### Parameters

These parameters are displayed in the web interface:

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

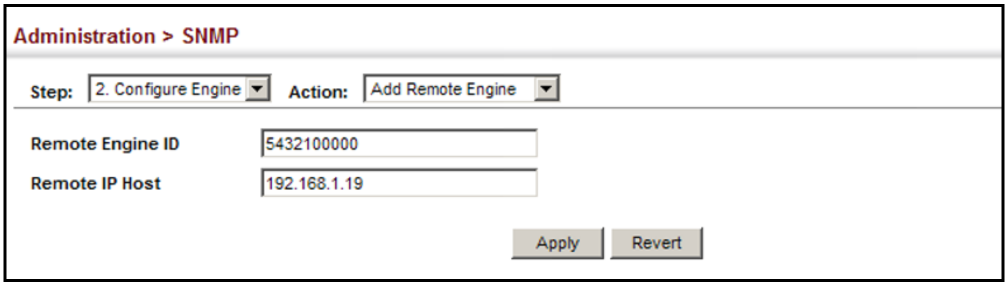
- **Remote IP Host** – The IP address of a remote management station which is using the specified engine ID.

### Web Interface

To configure a remote SNMP engine ID:

1. Click Administration, SNMP.
2. Select Configure Engine from the Step list.
3. Select Add Remote Engine from the Action list.
4. Enter an ID of a least 9 hexadecimal characters, and the IP address of the remote host.
5. Click Apply

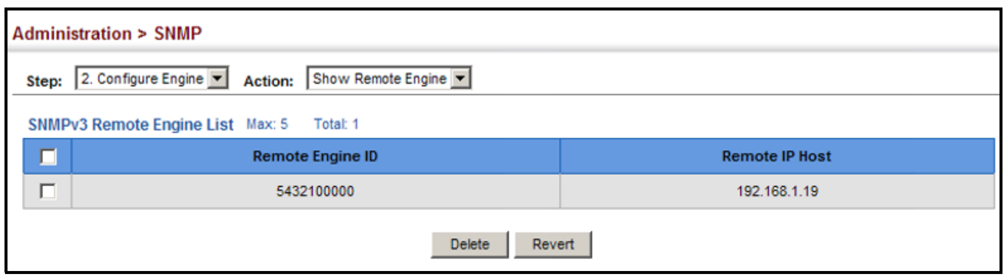
**Figure 15: Configuring a Remote Engine ID for SNMP**




To show the remote SNMP engine IDs:

1. Click Administration, SNMP.
2. Select Configure Engine from the Step list.
3. Select Show Remote Engine from the Action list.

**Figure 16: Showing Remote Engine IDs for SNMP**




## Setting SNMPv3 Views

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

### CLI REFERENCES

■ "snmp-server view" on page 669

### PARAMETERS

These parameters are displayed in the web interface:

*Add View*

■ **View Name** – The name of the SNMP view. (Range: 1-64 characters)

■ **OID Subtree** – Specifies the initial object identifier of a branch within the MIB tree. Wild cards can be used to mask a specific portion of the OID string. Use the Add OID Subtree page to configure additional object identifiers.

■ **Type** – Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view.

*Add OID Subtree*

■ **View Name** – Lists the SNMP views configured in the Add View page.

■ **OID Subtree** – Adds an additional object identifier of a branch within the MIB tree to the selected View. Wild cards can be used to mask a specific portion of the OID string.

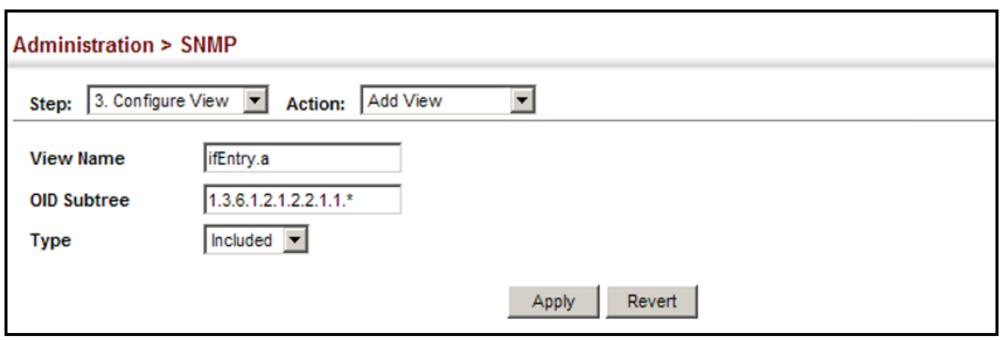
■ **Type** – Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view.

### WEB INTERFACE

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

1. Click Administration, SNMP.
2. Select Configure View from the Step list.
3. Select Add View from the Action list.
4. Enter a view name and specify the initial OID subtree in the switch's MIB database to be included or excluded in the view. Use the Add OID Subtree page to add additional object identifier branches to the view.
5. Click Apply

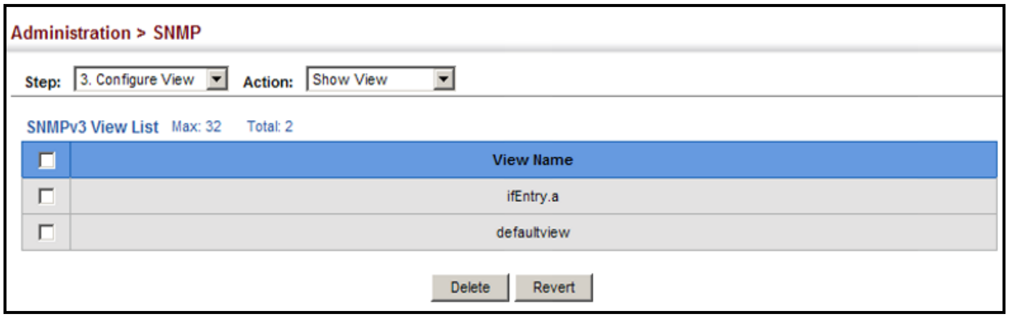
**Figure 17: Creating an SNMP View**




To show the SNMP views of the switch's MIB database:

1. Click Administration, SNMP.
2. Select Configure View from the Step list.
3. Select Show View from the Action list.

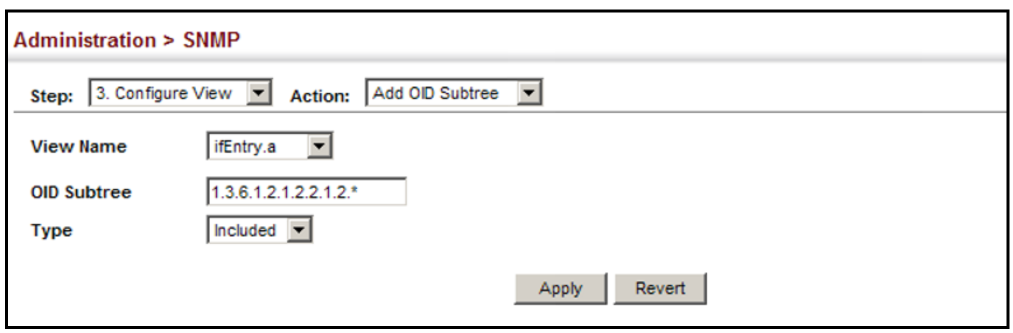
**Figure 18: Showing SNMP Views**




To add an object identifier to an existing SNMP view of the switch's MIB database:

1. Click Administration, SNMP.
2. Select Configure View from the Step list.
3. Select Add OID Subtree from the Action list.
4. Select a view name from the list of existing views, and specify an additional OID subtree in the switch's MIB database to be included or excluded in the view.
5. Click Apply

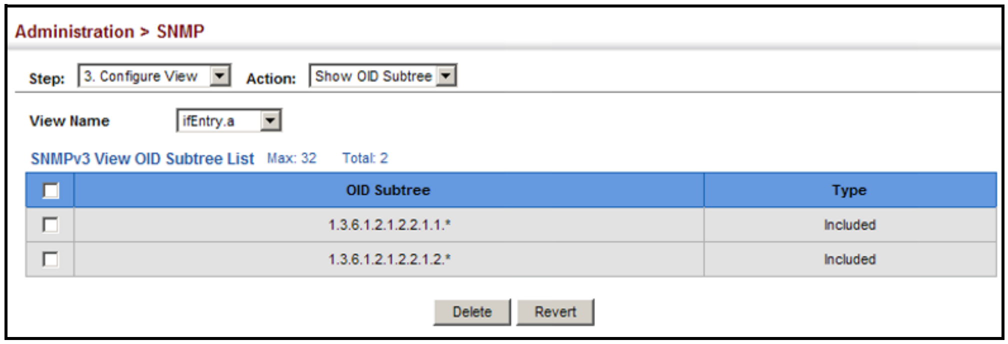
**Figure 19: Adding an OID Subtree to an SNMP View**




To show the OID branches configured for the SNMP views of the switch's MIB database:

1. Click Administration, SNMP.
2. Select Configure View from the Step list.
3. Select Show OID Subtree from the Action list.
4. Select a view name from the list of existing views.

**Figure 20: Showing the OID Subtree Configured for SNMP Views**




## Configuring SNMPv3 Groups

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

### CLI REFERENCES

■"show snmp group" on page 671

### PARAMETERS

These parameters are displayed in the web interface:

■**Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)

■**Security Model** – The user security model; SNMP v1, v2c or v3.

■**Security Level** – The following security levels are only used for the groups assigned to the SNMP security model:

- **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications. (This is the default security level.)
- **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.
- **AuthPriv** – SNMP communications use both authentication and encryption.

■**Read View** – The configured view for read access. (Range: 1-64 characters)

■**Write View** – The configured view for write access. (Range: 1-64 characters)

■**Notify View** – The configured view for notifications. (Range: 1-64 characters)

**Table 7: Supported Notification Messages**

| Model | Level | Group |
|---|---|---|
| *RFC 1493 Traps* | | |
| newRoot | 1.3.6.1.2.1.17.0.1 | The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer immediately subsequent to its election. |
| topologyChange | 1.3.6.1.2.1.17.0.2 | A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Discarding state. The trap is not sent if a newRoot trap is sent for the same transition. |
| *SNMPv2 Traps* | | |
| coldStart | 1.3.6.1.6.3.1.1.5.1 | A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered. |
| warmStart | 1.3.6.1.6.3.1.1.5.2 | A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered. |
| linkDown[1] | 1.3.6.1.6.3.1.1.5.3 | A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus. |
| linkUp* | 1.3.6.1.6.3.1.1.5.4 | A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus. |
| authenticationFailure* | 1.3.6.1.6.3.1.1.5.5 | An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated. |
| *RMON Events (V2)* | | |
| risingAlarm | 1.3.6.1.2.1.16.0.1 | The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps. |
| fallingAlarm | 1.3.6.1.2.1.16.0.2 | The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps. |
| *Private Traps* | | |
| swPowerStatusChangeTrap | 1.3.6.1.4.1.259.10.1.1.2.1.0.1 | This trap is sent when the power state changes. |
| swPortSecurityTrap | 1.3.6.1.4.1.259.10.1.1.2.1.0.36 | This trap is sent when the port is being intruded. This trap will only be sent when the portSecActionTrap is enabled. |
| swIpFilterRejectTrap | 1.3.6.1.4.1.259.10.1.1.2.1.0.40 | This trap is sent when an incorrect IP address is rejected by the IP Filter. |
| swSmtpConnFailureTrap | 1.3.6.1.4.1.259.10.1.1.2.1.0.41 | This trap is triggered if the SMTP system cannot open a connection to the mail server successfully. |

**Table 7: Supported Notification Messages (Continued)**

| Model | Level | Group |
|---|---|---|
| swMainBoardVerMismatchNotificaiton | 1.3.6.1.4.1.259.10.1.1.2.1.0.56 | This trap is sent when the slave board version is mismatched with the master board version. This trap binds two objects, the first object indicates the master version, whereas the second represents the slave version. |
| swAtcBcastStormAlarmFireTrap | 1.3.6.1.4.1.259.10.1.1.2.1.0.70 | When broadcast traffic is detected as a storm, this trap is fired. |
| swAtcBcastStormAlarmClearTrap | 1.3.6.1.4.1.259.10.1.1.2.1.0.71 | When a broadcast storm is detected as normal traffic, this trap is fired. |
| swAtcBcastStormTcApplyTrap | 1.3.6.1.4.1.259.10.1.1.2.1.0.72 | When ATC is activated, this trap is fired. |
| swAtcBcastStormTcReleaseTrap | 1.3.6.1.4.1.259.10.1.1.2.1.0.73 | When ATC is released, this trap is fired. |
| swAtcMcastStormAlarmFireTrap | 1.3.6.1.4.1.259.10.1.1.2.1.0.74 | When multicast traffic is detected as the storm, this trap is fired. |
| swAtcMcastStormAlarmClearTrap | 1.3.6.1.4.1.259.10.1.1.2.1.0.75 | When multicast storm is detected as normal traffic, this trap is fired. |
| swAtcMcastStormTcApplyTrap | 1.3.6.1.4.1.259.10.1.1.2.1.0.76 | When ATC is activated, this trap is fired. |
| swAtcMcastStormTcReleaseTrap | 1.3.6.1.4.1.259.10.1.1.2.1.0.77 | When ATC is released, this trap is fired. |
| swLoopbackDetectionTrap | 1.3.6.1.4.1.259.10.1.1.2.1.0.95 | This trap will be sent when loopback BPDUs have been detected. |
| networkAccessPortLinkDetectionTrap | 1.3.6.1.4.1.259.10.1.1.2.1.0.96 | This trap is sent when a networkAccessPortLinkDetection event is triggered. |
| swCpuUtiRisingNotification | 1.3.6.1.4.1.259.10.1.1.2.1.0.107 | This notification indicates that the CPU utilization crossed cpuUtiRisingThreshold. |
| swCpuUtiFallingNotification | 1.3.6.1.4.1.259.10.1.1.2.1.0.108 | This notification indicates that the CPU utilization crossed cpuUtiFallingThreshold. |
| swMemoryUtiRisingThresholdNotification | 1.3.6.1.4.1.259.10.1.1.2.1.0.109 | This notification indicates that the memory utilization crossed memoryUtiRisingThreshold. |
| swMemoryUtiFallingThresholdNotification | 1.3.6.1.4.1.259.10.1.1.2.1.0.110 | This notification indicates that the memory utilization crossed memoryUtiFallingThreshold. |
| swLoginFailureTrap | 1.3.6.1.4.1.259.10.1.1.2.1.0.139 | This trap is sent when login fails via console, telnet, or web. |
| swLoginSucceedTrap | 1.3.6.1.4.1.259.10.1.1.2.1.0.140 | This trap is sent when login succeeds via console, telnet, or web. |

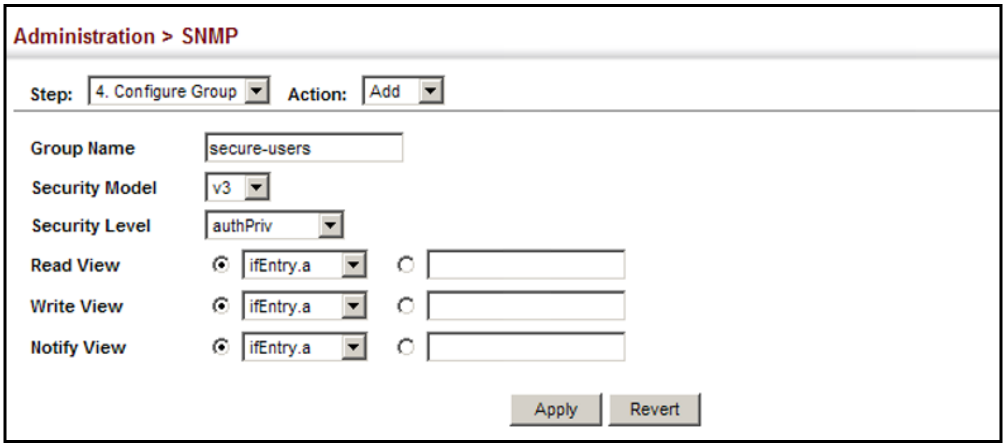
1. These are legacy notifications and therefore must be enabled in conjunction with the corresponding traps on the SNMP Configuration menu.

### WEB INTERFACE

To configure an SNMP group:

1. Click Administration, SNMP.
2. Select Configure Group from the Step list.
3. Select Add from the Action list.
4. Enter a group name, assign a security model and level, and then select read, write, and notify views.
5. Click Apply

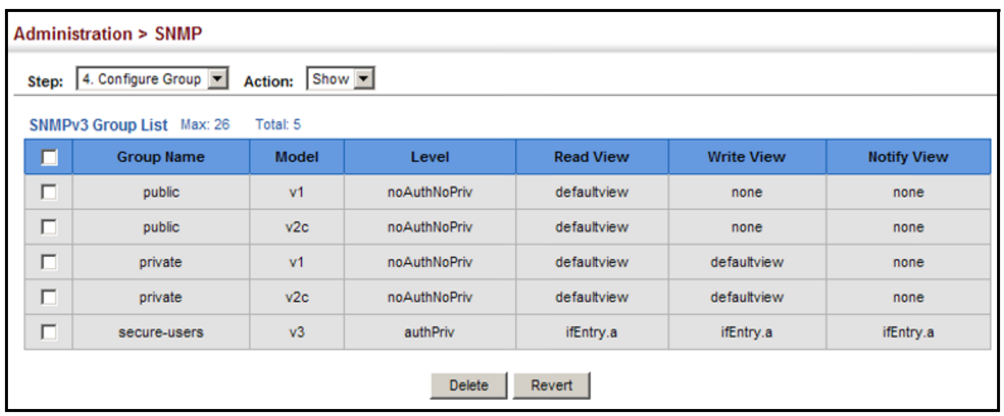
**Figure 21: Creating an SNMP Group**




To show SNMP groups:

1. Click Administration, SNMP.
2. Select Configure Group from the Step list.
3. Select Show from the Action list.

**Figure 22: Showing SNMP Groups**




## Setting Community Access Strings

Use the Administration > SNMP (Configure User - Add Community) page to configure up to five community strings authorized for management access by clients using SNMP v1 and v2c. For security reasons, you should consider removing the default strings.

### CLI REFERENCES

■ "snmp-server community" on page 660

### PARAMETERS

These parameters are displayed in the web interface:

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

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

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

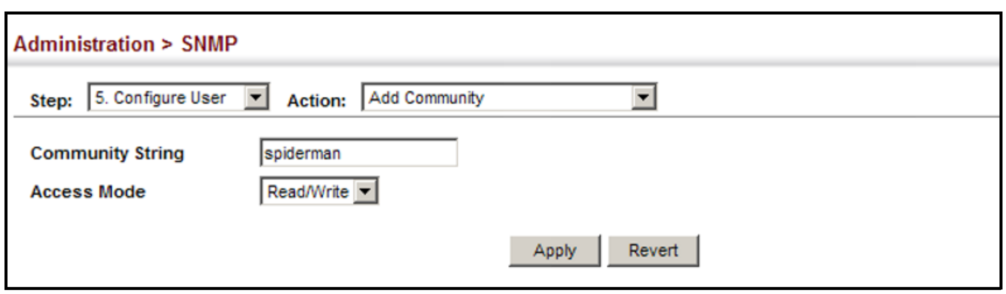
- **Read-Only** – Authorized management stations are only able to retrieve MIB objects.
- **Read/Write** – Authorized management stations are able to both retrieve and modify MIB objects.

### WEB INTERFACE

To set a community access string:

1. Click Administration, SNMP.
2. Select Configure User from the Step list.
3. Select Add Community from the Action list.
4. Add new community strings as required, and select the corresponding access rights from the Access Mode list.
5. Click Apply

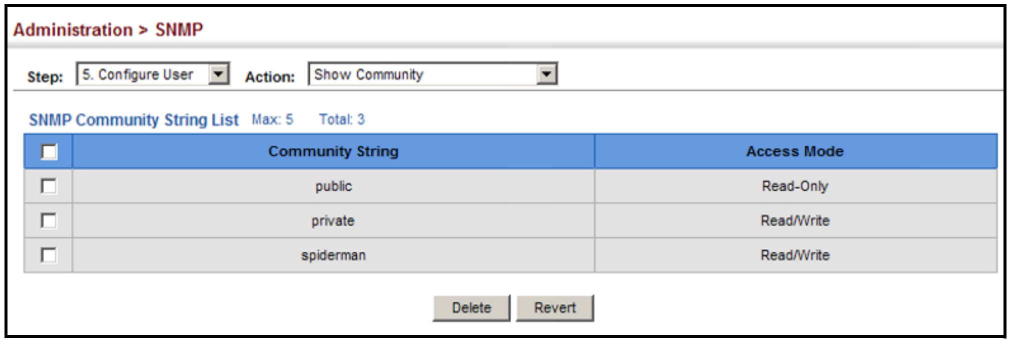
**Figure 23: Setting Community Access Strings**




To show the community access strings:

1. Click Administration, SNMP.
2. Select Configure User from the Step list.
3. Select Show Community from the Action list.

**Figure 24: Showing Community Access Strings**




## Configuring Local SNMPv3 Users

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

### CLI REFERENCES

- "snmp-server user" on page 668

### PARAMETERS

These parameters are displayed in the web interface:

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

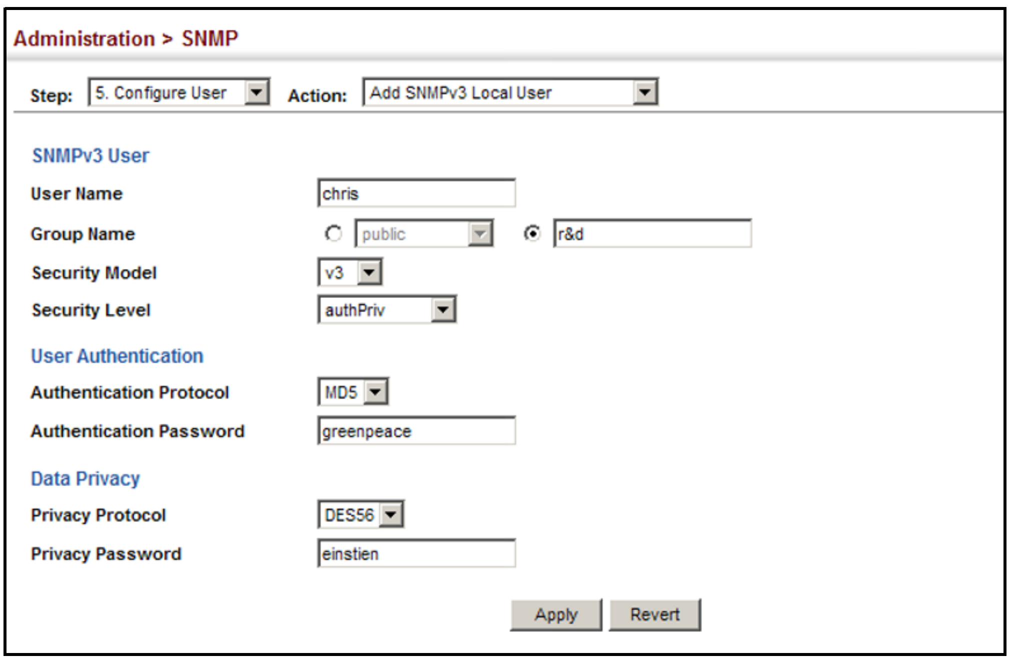
■**Privacy Password** – A minimum of eight plain text characters is required.

### WEB INTERFACE

To configure a local SNMPv3 user:

1. Click Administration, SNMP.
2. Select Configure User from the Step list.
3. Select Add SNMPv3 Local User from the Action list.
4. Enter a name and assign it to a group. If the security model is set to SNMPv3 and the security level is authNoPriv or authPriv, then an authentication protocol and password must be specified. If the security level is authPriv, a privacy password must also be specified.
5. Click Apply

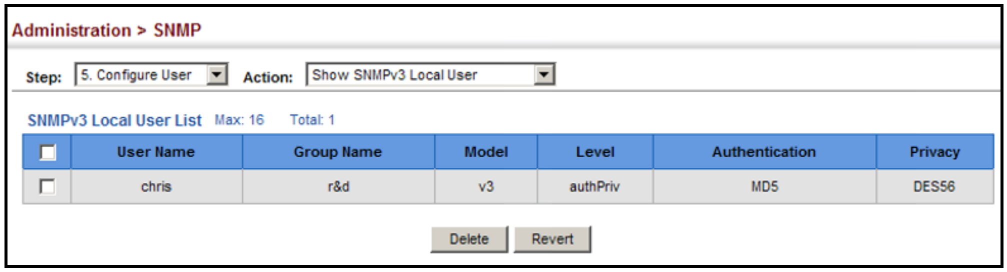
**Figure 25: Configuring Local SNMPv3 Users**




To show local SNMPv3 users:

1. Click Administration, SNMP.
2. Select Configure User from the Step list.
3. Select Show SNMPv3 Local User from the Action list.

**Figure 26: Showing Local SNMPv3 Users**




## Configuring Remote SNMPv3 Users

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

### CLI REFERENCES

- "snmp-server user" on page 668

### COMMAND USAGE

- To grant management access to an SNMPv3 user on a remote device, you must first specify the engine identifier for the SNMP agent on the remote device where the user resides. The remote engine ID is used to compute the security digest for authentication and encryption of packets passed between the switch and the remote user. (See "Specifying Trap Managers" on page 360 and "Specifying a Remote Engine ID" on page 347.)

### PARAMETERS

These parameters are displayed in the web interface:

- **User Name** – The name of user connecting to the SNMP agent. (Range: 1-32 characters)

- **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)

- **Remote IP** – The Internet address of the remote device where the user resides.

- **Security Model** – The user security model; SNMP v1, v2c or v3. (Default: v3)

- **Security Level** – The following security levels are only used for the groups assigned to the SNMP security model:

  - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications. (This is the default security level.)

  - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.

  - **AuthPriv** – SNMP communications use both authentication and encryption.

- **Authentication Protocol** – The method used for user authentication. (Options: MD5, SHA; Default: MD5)

- **Authentication Password** – A minimum of eight plain text characters is required.

- **Privacy Protocol** – The encryption algorithm use for data privacy; only 56-bit DES is currently available.

- **Privacy Password** – A minimum of eight plain text characters is required.

### WEB INTERFACE

To configure a remote SNMPv3 user:

1. Click Administration, SNMP.

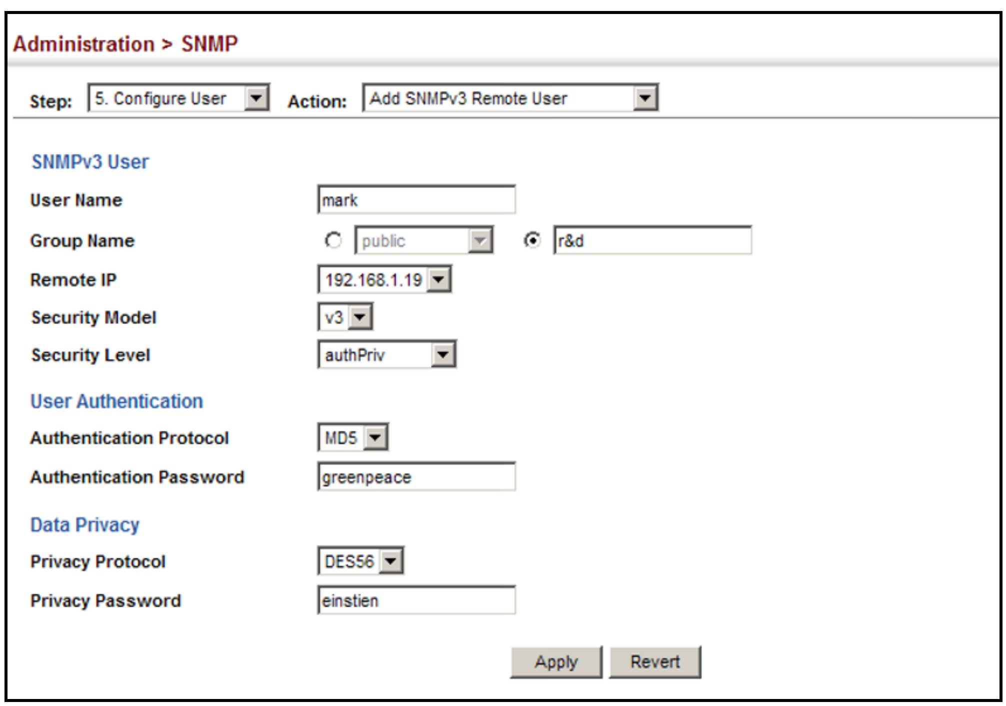
2. Select Configure User from the Step list.

3. Select Add SNMPv3 Remote User from the Action list.

4. Enter a name and assign it to a group. Enter the IP address to identify the source of SNMPv3 inform messages sent from the local switch. If the security model is set to SNMPv3 and the security level is authNoPriv or authPriv, then an authentication protocol and password must be specified. If the security level is authPriv, a privacy password must also be specified.

5. Click Apply.

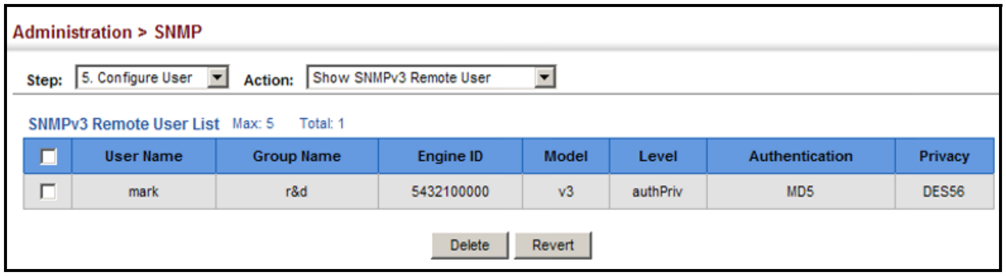
**Figure 27: Configuring Remote SNMPv3 Users**



To show remote SNMPv3 users:

1. Click Administration, SNMP.
2. Select Configure User from the Step list.
3. Select Show SNMPv3 Remote User from the Action list.

**Figure 28: Showing Remote SNMPv3 Users**




## Specifying Trap Managers

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

### CLI References

■ "snmp-server host" on page 664
■ "snmp-server enable traps" on page 663

### Command Usage

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

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

1. Enable the SNMP agent (page 345).
2. Create a view with the required notification messages (page 348).
3. Configure the group (matching the community string specified on the Configure Trap - Add page) to include the required notify view (page 351).
4. Enable trap informs as described in the following pages.

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

1. Enable the SNMP agent (page 345).

2. Create a local SNMPv3 user to use in the message exchange process (page 356). If the user specified in the trap configuration page does not exist, an SNMPv3 group will be automatically created using the name of the specified local user, and default settings for the read, write, and notify view.
3. Create a view with the required notification messages (page 348).
4. Create a group that includes the required notify view (page 351).
5. Enable trap informs as described in the following pages.

### PARAMETERS

These parameters are displayed in the web interface:

*SNMP Version 1*

- **IP Address** – IP address of a new management station to receive notification message (i.e., the targeted recipient).
- **Version** – Specifies whether to send notifications as SNMP v1, v2c, or v3 traps. (Default: v1)
- **Community String** – Specifies a valid community string for the new trap manager entry. (Range: 1-32 characters, case sensitive)

  Although you can set this string in the Configure Trap – Add page, we recommend defining it in the Configure User – Add Community page.
- **UDP Port** – Specifies the UDP port number used by the trap manager. (Default: 162)

*SNMP Version 2c*

- **IP Address** – IP address of a new management station to receive notification message (i.e., the targeted recipient).
- **Version** – Specifies whether to send notifications as SNMP v1, v2c, or v3 traps.
- **Notification Type**
  - **Traps** – Notifications are sent as trap messages.
  - **Inform** – Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)
    - **Timeout** – The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)
    - **Retry times** – The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)
- **Community String** – Specifies a valid community string for the new trap manager entry. (Range: 1-32 characters, case sensitive)

Although you can set this string in the Configure Trap – Add page, we recommend defining it in the Configure User – Add Community page.

- **UDP Port** – Specifies the UDP port number used by the trap manager. (Default: 162)

*SNMP Version 3*

- **IP Address** – IP address of a new management station to receive notification message (i.e., the targeted recipient).
- **Version** – Specifies whether to send notifications as SNMP v1, v2c, or v3 traps.
- **Notification Type**
  - **Traps** – Notifications are sent as trap messages.
  - **Inform** – Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)
    - **Timeout** – The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)
    - **Retry times** – The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)
- **Local User Name** – The name of a local user which is used to identify the source of SNMPv3 trap messages sent from the local switch. (Range: 1-32 characters)

  If an account for the specified user has not been created (page 356), one will be automatically generated.
- **Remote User Name** – The name of a remote user which is used to identify the source of SNMPv3 inform messages sent from the local switch. (Range: 1-32 characters)

  If an account for the specified user has not been created (page 358), one will be automatically generated.
- **UDP Port** – Specifies the UDP port number used by the trap manager. (Default: 162)
- **Security Level** – When trap version 3 is selected, you must specify one of the following security levels. (Default: noAuthNoPriv)
  - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications.
  - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.
  - **AuthPriv** – SNMP communications use both authentication and encryption.

### WEB INTERFACE

To configure trap managers:

1. Click Administration, SNMP.
2. Select Configure Trap from the Step list.
3. Select Add from the Action list.
4. Fill in the required parameters based on the selected SNMP version.
5. Click Apply

**Figure 29: Configuring Trap Managers** (SNMPv1)

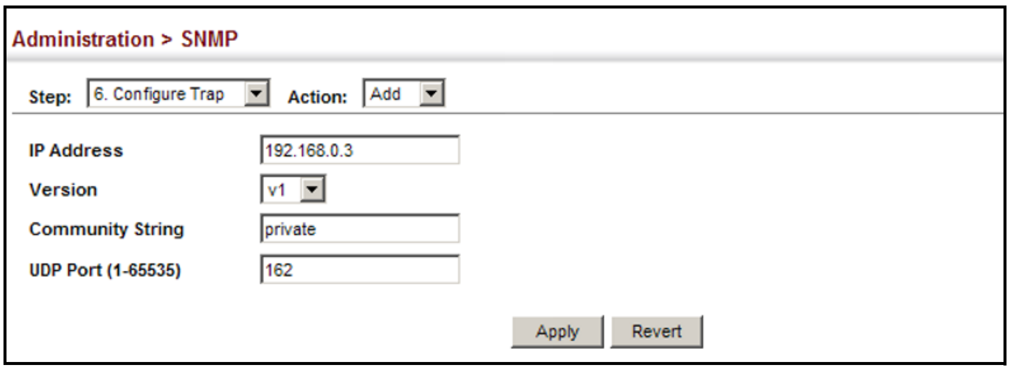



**Figure 30: Configuring Trap Managers** (SNMPv2c)

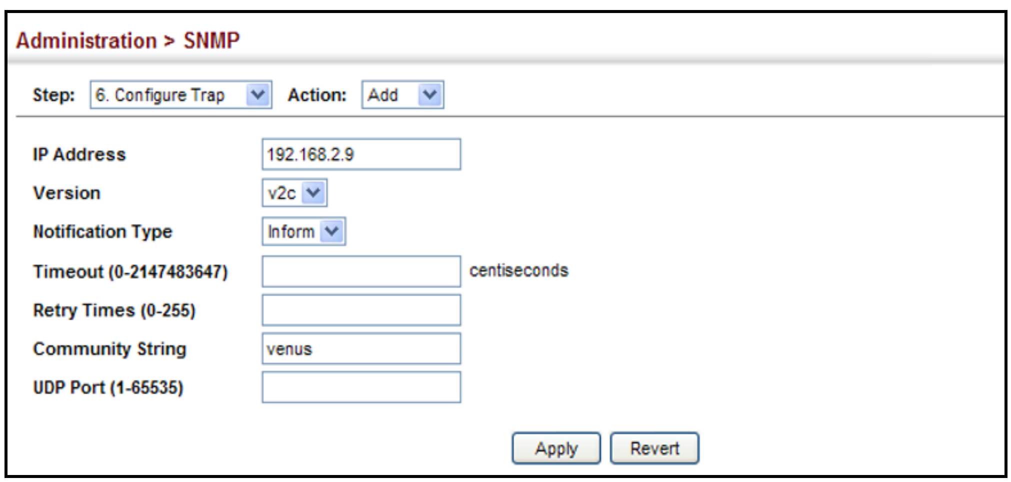
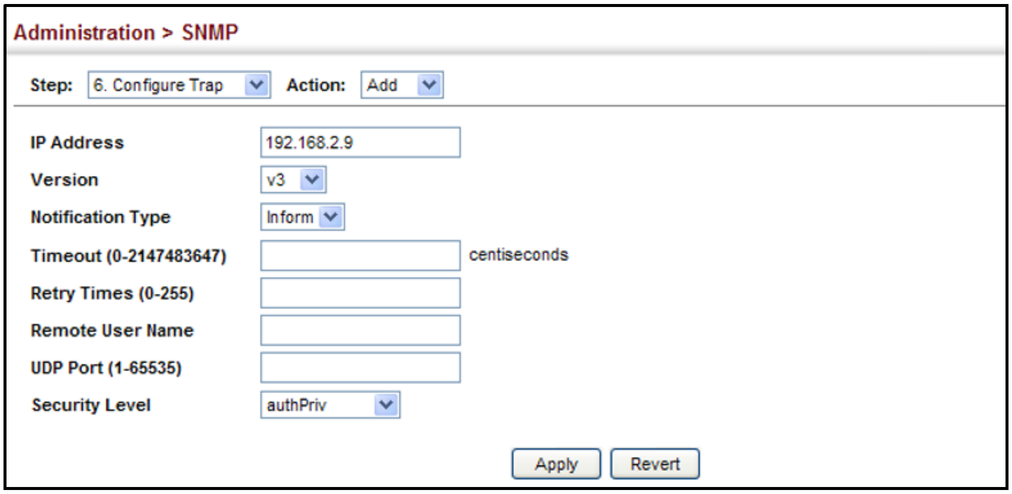


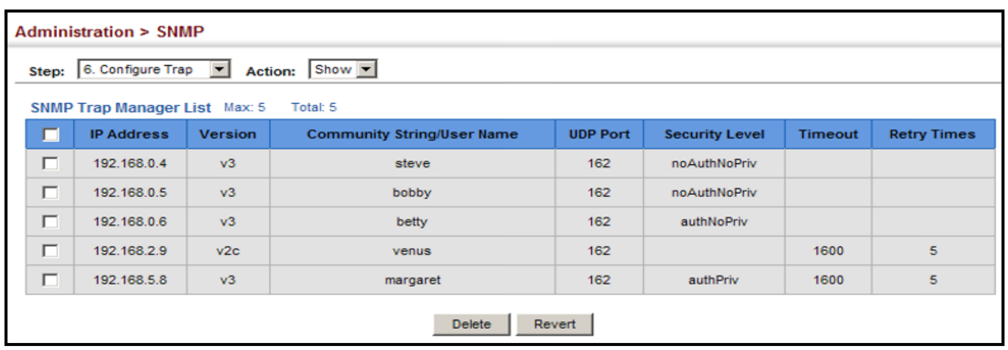
**Figure 31: Configuring Trap Managers** (SNMPv3)




To show configured trap managers:

1. Click Administration, SNMP.
2. Select Configure Trap from the Step list.
3. Select Show from the Action list.

**Figure 32: Showing Trap Managers**




## REMOTE MONITORING

Remote Monitoring allows a remote device to collect information or respond to specified events on an independent basis. This switch is an RMON-capable device which can independently perform a wide range of tasks, significantly reducing network management traffic. It can continuously run diagnostics and log information on network performance. If an event is triggered, it can automatically notify the network administrator of a failure and provide historical information about the event. If it cannot connect to the management agent, it will continue to perform any specified tasks and pass data back to the management station the next time it is contacted.

The switch supports mini-RMON, which consists of the Statistics, History, Event and Alarm groups. When RMON is enabled, the system gradually builds up information about its physical interfaces, storing this information in the relevant RMON database group. A management agent then periodically communicates with the switch using the SNMP protocol. However, if the switch encounters a critical event, it can automatically send a trap message to the management agent which can then respond to the event if so configured.

## Configuring RMON Alarms

Use the Administration > RMON (Configure Global - Add - Alarm) page to define specific criteria that will generate response events. Alarms can be set to test data over any specified time interval, and can monitor absolute or changing values (such as a statistical counter reaching a specific value, or a statistic changing by a certain amount over the set interval). Alarms can be set to respond to rising or falling thresholds. (However, note that after an alarm is triggered it will not be triggered again until the statistical value crosses the opposite bounding threshold and then back across the trigger threshold.

### CLI REFERENCES

- "Remote Monitoring Commands" on page 677

### COMMAND USAGE

- If an alarm is already defined for an index, the entry must be deleted before any changes can be made.

### PARAMETERS

These parameters are displayed in the web interface:

- **Index** – Index to this entry. (Range: 1-65535)

- **Status** – The status of this alarm entry. (Displayed data includes: Valid, createRequest, underCreation, or Invalid)

- **Variable** – The object identifier of the MIB variable to be sampled. Only variables of the type etherStatsEntry.n.n may be sampled.

  Note that etherStatsEntry.n uniquely defines the MIB variable, and etherStatsEntry.n.n defines the MIB variable, plus the etherStatsIndex. For example, 1.3.6.1.2.1.16.1.1.1.6.1 denotes etherStatsBroadcastPkts, plus the etherStatsIndex of 1.

- **Interval** – The polling interval. (Range: 1-31622400 seconds)

- **Sample Type** – Tests for absolute or relative changes in the specified variable.

  - **Absolute** – The variable is compared directly to the thresholds at the end of the sampling period.

  - **Delta** – The last sample is subtracted from the current value and the difference is then compared to the thresholds.

- **Rising Threshold** – If the current value is greater than or equal to the rising threshold, and the last sample value was less than this threshold, then an alarm will be generated. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the rising threshold, reaches the falling threshold, and again moves back up to the rising threshold. (Range: 1-65535)

- **Rising Event Index** – The index of the event to use if an alarm is triggered by monitored variables reaching or crossing above the rising threshold. If there is no corresponding entry in the event control table, then no event will be generated. (Range: 1-65535)

- **Falling Threshold** – If the current value is less than or equal to the falling threshold, and the last sample value was greater than this threshold, then an alarm will be generated. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the falling threshold, reaches the rising threshold, and again moves back down to the failing threshold. (Range: 1-65535)

- **Falling Event Index** – The index of the event to use if an alarm is triggered by monitored variables reaching or crossing below the falling threshold. If there is no corresponding entry in the event control table, then no event will be generated. (Range: 1-65535)

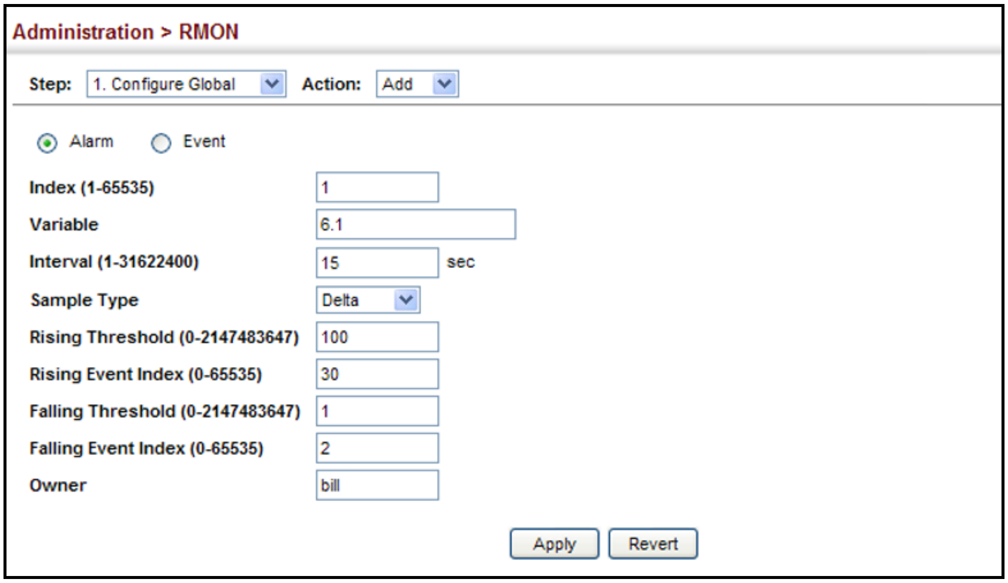
- **Owner** – Name of the person who created this entry. (Range: 1-127 characters)

#### WEB INTERFACE

To configure an RMON alarm:

1. Click Administration, RMON.
2. Select Configure Global from the Step list.
3. Select Add from the Action list.
4. Click Alarm.
5. Enter an index number, the MIB object to be polled (etherStatsEntry.n.n), the polling interval, the sample type, the thresholds, and the event to trigger.
6. Click Apply

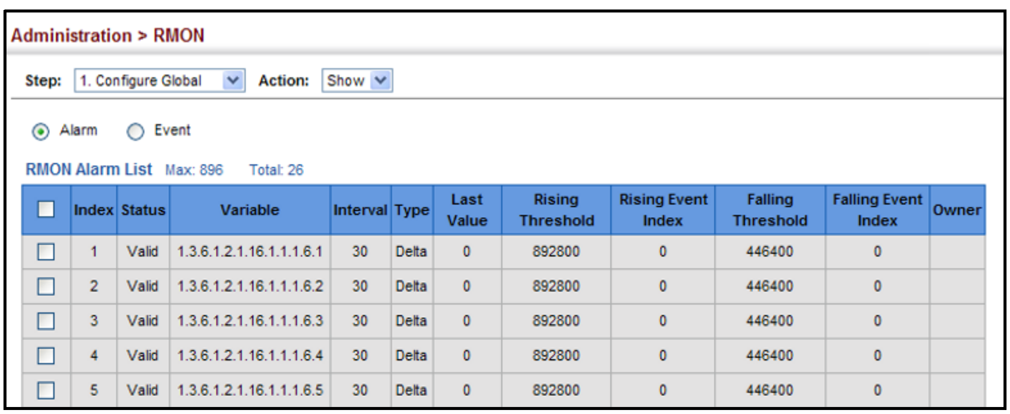
**Figure 33: Configuring an RMON Alarm**




To show configured RMON alarms:

1. Click Administration, RMON.
2. Select Configure Global from the Step list.
3. Select Show from the Action list.
4. Click Alarm.

**Figure 34: Showing Configured RMON Alarms**




| | Index | Status | Variable | Interval | Type | Last Value | Rising Threshold | Rising Event Index | Falling Threshold | Falling Event Index | Owner |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | Valid | 1.3.6.1.2.1.16.1.1.1.6.1 | 30 | Delta | 0 | 892800 | 0 | 446400 | 0 | |
| | 2 | Valid | 1.3.6.1.2.1.16.1.1.1.6.2 | 30 | Delta | 0 | 892800 | 0 | 446400 | 0 | |
| | 3 | Valid | 1.3.6.1.2.1.16.1.1.1.6.3 | 30 | Delta | 0 | 892800 | 0 | 446400 | 0 | |
| | 4 | Valid | 1.3.6.1.2.1.16.1.1.1.6.4 | 30 | Delta | 0 | 892800 | 0 | 446400 | 0 | |
| | 5 | Valid | 1.3.6.1.2.1.16.1.1.1.6.5 | 30 | Delta | 0 | 892800 | 0 | 446400 | 0 | |

## Configuring RMON Events

Use the Administration > RMON (Configure Global - Add - Event) page to set the action to take when an alarm is triggered. The response can include logging the alarm or sending a message to a trap manager. Alarms and corresponding events provide a way of immediately responding to critical network problems.

### CLI REFERENCES

- "Remote Monitoring Commands" on page 677

### COMMAND USAGE

- If an alarm is already defined for an index, the entry must be deleted before any changes can be made.
- One default event is configured as follows:

  event Index = 1
  Description: RMON_TRAP_LOG
  Event type: log & trap
  Event community name is public
  Owner is RMON_SNMP

### PARAMETERS

These parameters are displayed in the web interface:

- **Index** – Index to this entry. (Range: 1-65535)
- **Type** – Specifies the type of event to initiate:
  - **None** – No event is generated.
  - **Log** – Generates an RMON log entry when the event is triggered. Log messages are processed based on the current configuration settings for event logging (see "System Log Configuration" on page 325).
  - **Trap** – Sends a trap message to all configured trap managers (see "Specifying Trap Managers" on page 360).
  - **Log and Trap** – Logs the event and sends a trap message.
- **Community** – A password-like community string sent with the trap operation to SNMP v1 and v2c hosts.

  Although the community string can be set on this configuration page, it is recommended that it be defined on the SNMP trap configuration page (see "Setting Community Access Strings" on page 354) prior to configuring it here. (Range: 1-32 characters)
- **Description** – A comment that describes this event. (Range: 1-127 characters)
- **Owner** – Name of the person who created this entry. (Range: 1-127 characters)

### WEB INTERFACE

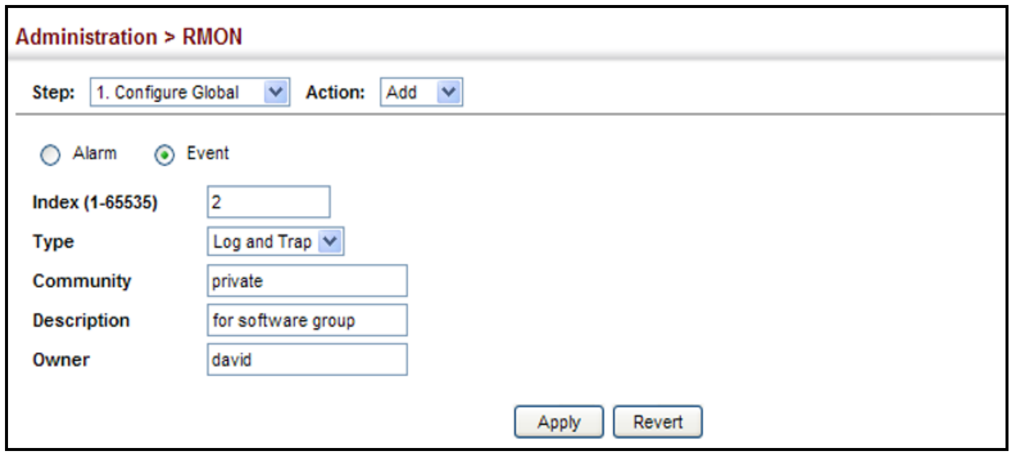
To configure an RMON event:

1. Click Administration, RMON.
2. Select Configure Global from the Step list.
3. Select Add from the Action list.
4. Click Event.

5. Enter an index number, the type of event to initiate, the community string to send with trap messages, the name of the person who created this event, and a brief description of the event.

6. Click Apply

**Figure 35: Configuring an RMON Event**




To show configured RMON events:

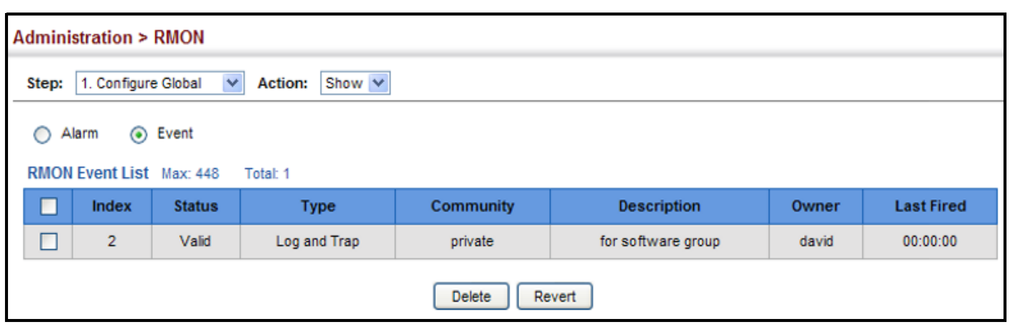
1. Click Administration, RMON.

2. Select Configure Global from the Step list.

3. Select Show from the Action list.

4. Click Event.

**Figure 36: Showing Configured RMON Events**




## Configuring RMON History Samples

Use the Administration > RMON (Configure Interface - Add - History) page to collect statistics on a physical interface to monitor network utilization, packet types, and errors. A historical record of activity can be used to track down intermittent problems. The record can be used to establish normal baseline activity, which may reveal problems associated with high traffic levels, broadcast storms, or other unusual events. It can also be used to predict network growth and plan for expansion before your network becomes too overloaded.

### CLI REFERENCES

- "Remote Monitoring Commands" on page 677

### COMMAND USAGE

- Each index number equates to a port on the switch.
- If history collection is already enabled on an interface, the entry must be deleted before any changes can be made.
- The information collected for each sample includes:

  input octets, packets, broadcast packets, multicast packets, undersize packets, oversize packets, fragments, jabbers, CRC alignment errors, collisions, drop events, and network utilization.

  For a description of the statistics displayed on the Show Details page, refer to "Showing Port or Trunk Statistics" on page 113.

### PARAMETERS

These parameters are displayed in the web interface:

- **Port** – The port number on the switch.
- **Index** - Index to this entry. (Range: 1-65535)
- **Interval** - The polling interval. (Range: 1-3600 seconds; Default: 1800 seconds)
- **Buckets** - The number of buckets requested for this entry. (Range: 1-65536; Default: 50)

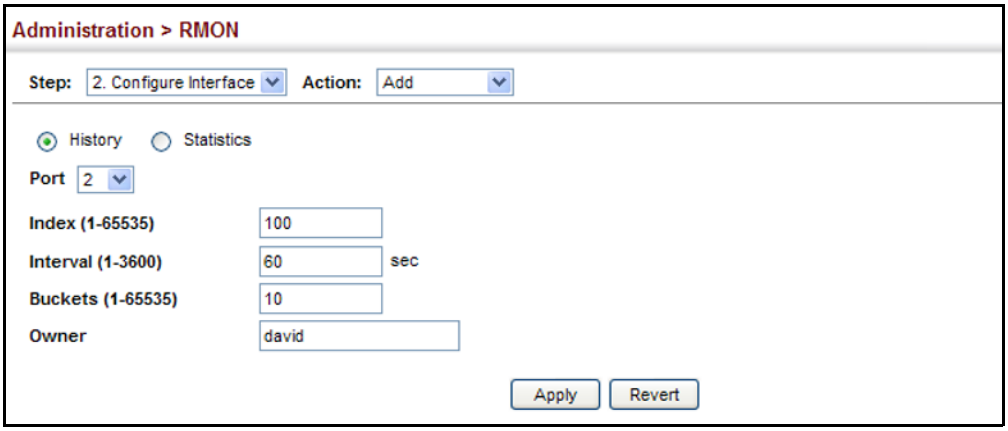
  The number of buckets granted are displayed on the Show page.
- **Owner** - Name of the person who created this entry. (Range: 1-127 characters)

### WEB INTERFACE

To periodically sample statistics on a port:

1. Click Administration, RMON.
2. Select Configure Interface from the Step list.
3. Select Add from the Action list.
4. Click History.
5. Select a port from the list as the data source.
6. Enter an index number, the sampling interval, the number of buckets to use, and the name of the owner for this entry.
7. Click Apply

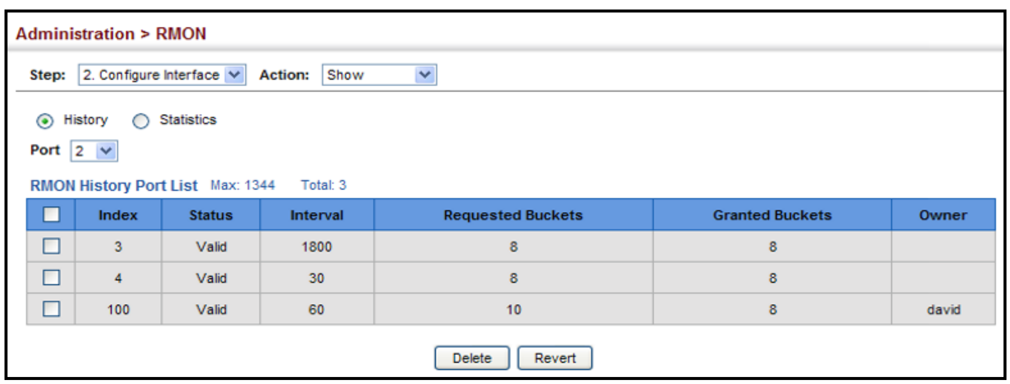
**Figure 37: Configuring an RMON History Sample**




To show configured RMON history samples:

1. Click Administration, RMON.
2. Select Configure Interface from the Step list.
3. Select Show from the Action list.
4. Select a port from the list.
5. Click History.

**Figure 38: Showing Configured RMON History Samples**

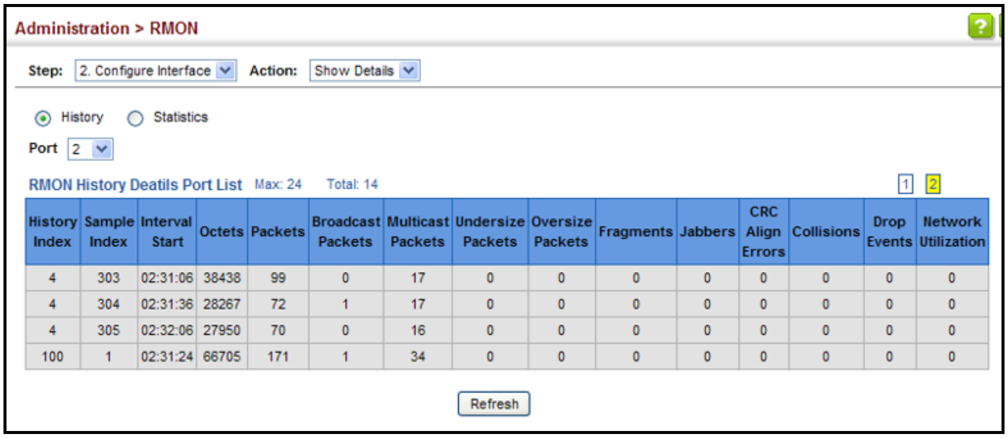



| | Index | Status | Interval | Requested Buckets | Granted Buckets | Owner |
|---|---|---|---|---|---|---|
| | 3 | Valid | 1800 | 8 | 8 | |
| | 4 | Valid | 30 | 8 | 8 | |
| | 100 | Valid | 60 | 10 | 8 | david |

To show collected RMON history samples:

1. Click Administration, RMON.
2. Select Configure Interface from the Step list.
3. Select Show Details from the Action list.
4. Select a port from the list.
5. Click History.

**Figure 39: Showing Collected RMON History Samples**




| History Index | Sample Index | Interval Start | Octets | Packets | Broadcast Packets | Multicast Packets | Undersize Packets | Oversize Packets | Fragments | Jabbers | CRC Align Errors | Collisions | Drop Events | Network Utilization |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 303 | 02:31:06 | 38438 | 99 | 0 | 17 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 304 | 02:31:36 | 28267 | 72 | 1 | 17 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 305 | 02:32:06 | 27950 | 70 | 0 | 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 100 | 1 | 02:31:24 | 66705 | 171 | 1 | 34 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

## Configuring RMON Statistical Samples

Use the Administration > RMON (Configure Interface - Add - Statistics) page to collect statistics on a port, which can subsequently be used to monitor the network for common errors and overall traffic rates.

### CLI References

■"Remote Monitoring Commands" on page 677

### Command Usage

■If statistics collection is already enabled on an interface, the entry must be deleted before any changes can be made.

■The information collected for each entry includes:

input octets, packets, broadcast packets, multicast packets, undersize packets, oversize packets, CRC alignment errors, jabbers, fragments, collisions, drop events, and frames of various sizes.

### Parameters

These parameters are displayed in the web interface:

■**Port** – The port number on the switch.

■**Index** - Index to this entry. (Range: 1-65535)

■**Owner** - Name of the person who created this entry. (Range: 1-127 characters)

### Web Interface

To enable regular sampling of statistics on a port:

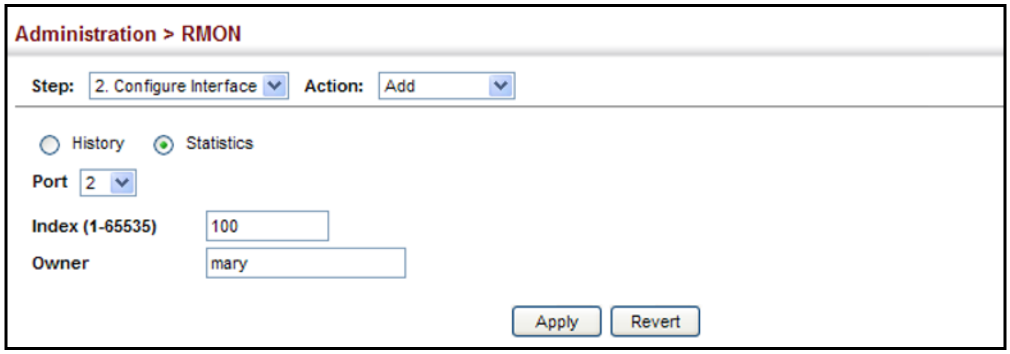
1. Click Administration, RMON.
2. Select Configure Interface from the Step list.
3. Select Add from the Action list.
4. Click Statistics.

5. Select a port from the list as the data source.

6. Enter an index number, and the name of the owner for this entry

7. Click Apply

**Figure 40: Configuring an RMON Statistical Sample**




To show configured RMON statistical samples:

1. Click Administration, RMON.

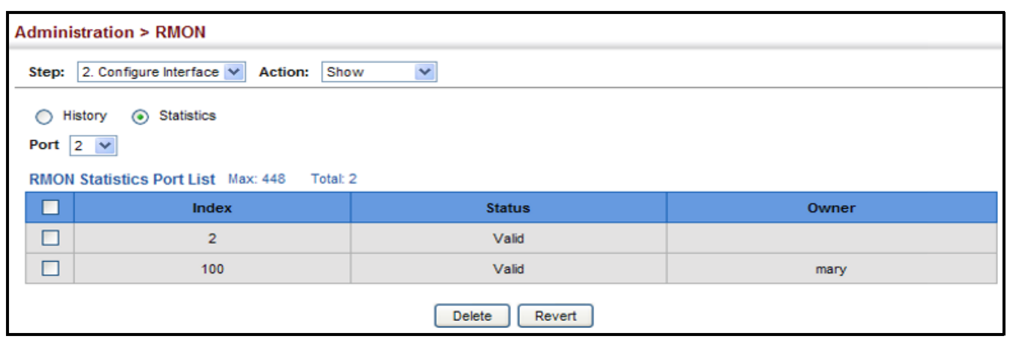
2. Select Configure Interface from the Step list.

3. Select Show from the Action list.

4. Select a port from the list.

5. Click Statistics.

**Figure 41: Showing Configured RMON Statistical Samples**




To show collected RMON statistical samples:

1. Click Administration, RMON.

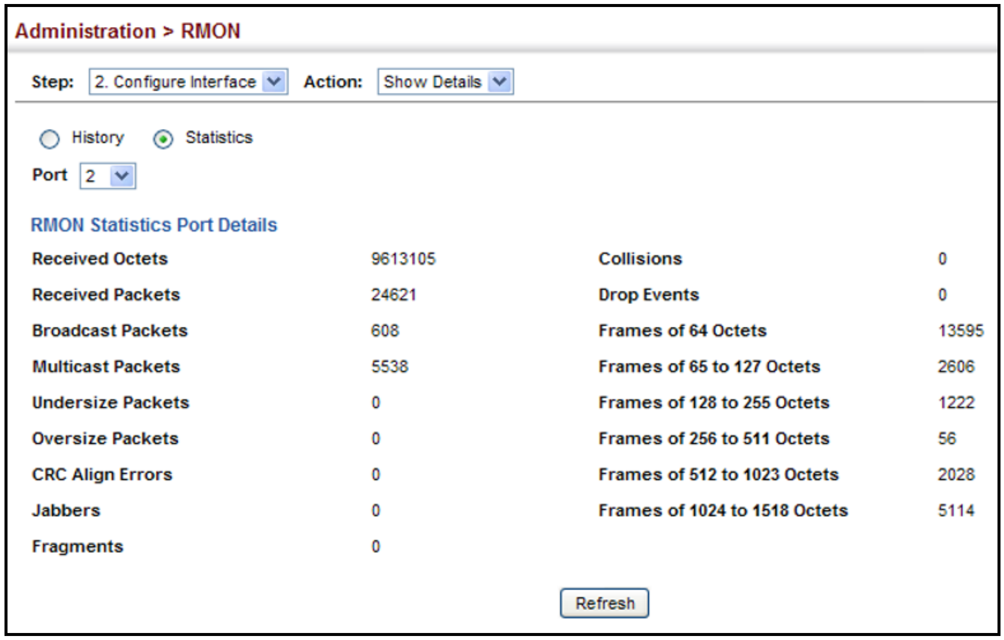
2. Select Configure Interface from the Step list.

3. Select Show Details from the Action list.

4. Select a port from the list.

**5.** Click Statistics.

**Figure 42: Showing Collected RMON Statistical Samples**




| | | | |
|---|---|---|---|
| Received Octets | 9613105 | Collisions | 0 |
| Received Packets | 24621 | Drop Events | 0 |
| Broadcast Packets | 608 | Frames of 64 Octets | 13595 |
| Multicast Packets | 5538 | Frames of 65 to 127 Octets | 2606 |
| Undersize Packets | 0 | Frames of 128 to 255 Octets | 1222 |
| Oversize Packets | 0 | Frames of 256 to 511 Octets | 56 |
| CRC Align Errors | 0 | Frames of 512 to 1023 Octets | 2028 |
| Jabbers | 0 | Frames of 1024 to 1518 Octets | 5114 |
| Fragments | 0 | | |

# 16 MULTICAST FILTERING

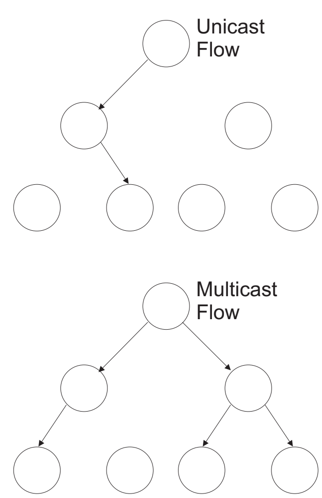
This chapter describes how to configure the following multicast services:

- Layer 2 IGMP – Configures snooping and query parameters.
- Filtering and Throttling – Filters specified multicast service, or throttling the maximum of multicast groups allowed on an interface.
- Layer 3 IGMP – Configures IGMP query used with multicast routing.
- Multicast VLAN Registration (MVR) – Configures a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, preserving security and data isolation.

## OVERVIEW

Multicasting is used to support real-time applications such as video conferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts that want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed on to the hosts which subscribed to this service.

**Figure 1: Multicast Filtering Concept**




This switch can use Internet Group Management Protocol (IGMP) to filter multicast traffic. IGMP Snooping can be used to passively monitor or “snoop” on exchanges between attached hosts and an IGMP-enabled device, most commonly a multicast router. In this way, the switch can discover the ports that want to join a multicast group, and set its filters accordingly.

If there is no multicast router attached to the local subnet, multicast traffic and query messages may not be received by the switch. In this case IGMP Query can be used to actively ask the attached hosts if they want to receive a specific multicast service. IGMP Query thereby identifies the ports containing hosts requesting to join the service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

The purpose of IP multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches, instead of flooding traffic to all ports in the subnet (VLAN).

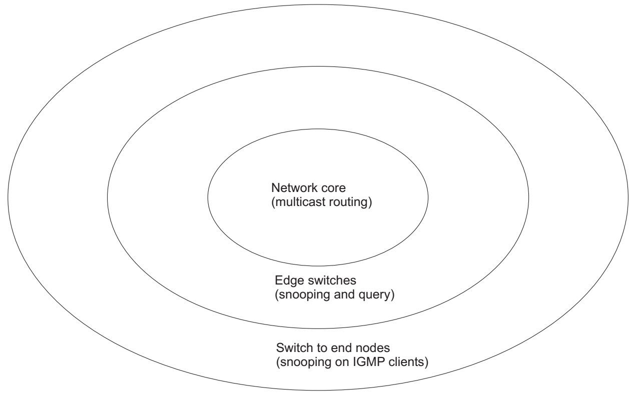
This switch not only supports IP multicast filtering by passively monitoring IGMP query, report messages and multicast routing probe messages to register end-stations as multicast group members, but also supports the Protocol Independent Multicasting (PIM) routing protocol required to forward multicast traffic to other subnets (page 1208).

You can also configure a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, preserving security and data isolation "Multicast VLAN Registration" on page 408.

## IGMP PROTOCOL

The Internet Group Management Protocol (IGMP) runs between hosts and their immediately adjacent multicast router/switch. IGMP is a multicast host registration protocol that allows any host to inform its local router that it wants to receive transmissions addressed to a specific multicast group. 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" (at Layer 3) 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. Based on the group membership information learned from IGMP, a router/switch can determine which (if any) multicast traffic needs to be forwarded to each of its ports. At Layer 3, multicast routers use this information, along with a multicast routing protocol such as Protocol Independent Multicasting (PIM), to support IP multicasting across the Internet. Note that IGMP neither alters nor routes IP multicast packets. A multicast routing protocol must be used to deliver IP multicast packets across different subnetworks. Therefore, when PIM routing is enabled for a subnet on the switch, IGMP is automatically enabled.

**Figure 2: IGMP Protocol**




## LAYER 2 IGMP (SNOOPING AND QUERY)

IGMP Snooping and Query – If multicast routing is not supported on other switches in your network, you can use IGMP Snooping and IGMP Query (page 379) to monitor IGMP service requests passing between multicast clients and servers, and dynamically configure the switch ports which need to forward multicast traffic. IGMP Snooping conserves bandwidth on network segments where no node has expressed interest in receiving a specific multicast service. For switches that do not support multicast routing, or where multicast routing is already enabled on other switches in the local network segment, IGMP Snooping is the only service required to support multicast filtering.

When using IGMPv3 snooping, service requests from IGMP Version 1, 2 or 3 hosts are all forwarded to the upstream router as IGMPv3 reports. The primary enhancement provided by IGMPv3 snooping is in keeping track of information about the specific multicast sources which downstream IGMPv3 hosts have requested or refused. The switch maintains information about both multicast groups and channels, where a group indicates a multicast flow for which the hosts have *not* requested a specific source (the only option for IGMPv1 and v2 hosts unless statically configured on the switch), and a channel indicates a flow for which the hosts have requested service from a specific source. For IGMPv1/v2 hosts, the source address of a channel is always null (indicating that any source is acceptable), but for IGMPv3 hosts, it may include a specific address when requested.

Only IGMPv3 hosts can request service from a specific multicast source. When downstream hosts request service from a specific source for a multicast service, these sources are all placed in the Include list, and traffic is forwarded to the hosts from each of these sources. IGMPv3 hosts may also request that service be forwarded from any source except for those specified. In this case, traffic is filtered from sources in the Exclude list, and forwarded from all other available sources.

**Note:** When the switch is configured to use IGMPv3 snooping, the snooping version may be downgraded to version 2 or version 1, depending on the version of the IGMP query packets detected on each VLAN.

**Note:** IGMP snooping will not function unless a multicast router port is enabled on the switch. This can accomplished in one of two ways. A static router port can be manually configured (see "Specifying Static Interfaces for a Multicast Router" on page 382). Using this method, the router port is never timed out, and will continue to function until explicitly removed. The other method relies on the switch to dynamically create multicast routing ports whenever multicast routing protocol packets or IGMP query packets are detected on a port.

**Note:** A maximum of up to 1024 multicast entries can be maintained for IGMP snooping and Multicast Routing when both of these features are enabled. Once the table is full, no new entries are learned. Any subsequent multicast traffic not found in the table is dropped if unregistered-flooding is disabled (default behavior) and no router port is configured in the attached VLAN, or flooded throughout the VLAN if unregistered-flooding is enabled (see "Configuring IGMP Snooping and Query Parameters" on page 379).

Static IGMP Router Interface – If IGMP snooping cannot locate the IGMP querier, you can manually designate a known IGMP querier (i.e., a multicast router/switch) connected over the network to an interface on your switch (page 382). 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 (page 384).

IGMP Snooping with Proxy Reporting – The switch supports last leave, and query suppression (as defined in DSL Forum TR-101, April 2006):

- Last Leave: Intercepts, absorbs and summarizes IGMP leaves coming from IGMP hosts. IGMP leaves are relayed upstream only when necessary, that is, when the last user leaves a multicast group.
- Query Suppression: Intercepts and processes IGMP queries in such a way that IGMP specific queries are never sent to client ports.

The only deviation from TR-101 is that report suppression, and the marking of IGMP traffic initiated by the switch with priority bits as defined in R-250 is not supported.

## Configuring IGMP Snooping and Query Parameters

Use the Multicast > IGMP Snooping > General page to configure the switch to forward multicast traffic intelligently. Based on the IGMP query and report messages, the switch forwards multicast traffic only to the ports that request it. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.

### CLI REFERENCES

■ "IGMP Snooping" on page 957

### COMMAND USAGE

■ **IGMP Snooping** – This switch can passively snoop on IGMP Query and Report packets transferred between IP multicast routers/switches and IP multicast host groups to identify the IP multicast group members. It simply monitors the IGMP packets passing through it, picks out the group registration information, and configures the multicast filters accordingly.

**NOTE:** If unknown multicast traffic enters a VLAN which has been configured with a router port, the traffic is forwarded to that port. However, if no router port exists on the VLAN, the traffic is dropped if unregistered-flooding is disabled (default behavior), or flooded throughout the VLAN if unregistered-flooding is enabled (see “Unregistered Data Flood” in the Command Attributes section).

■ **IGMP Querier** – A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected “querier” and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

**NOTE:** Multicast routers use this information from IGMP snooping and query reports, along with a multicast routing protocol such as PIM, to support IP multicasting across the Internet.

### PARAMETERS

These parameters are displayed in the web interface:

■ **IGMP Snooping Status** – When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is referred to as IGMP Snooping. (Default: Disabled)

When IGMP snooping is enabled globally, the per VLAN interface settings for IGMP snooping take precedence (see "Setting IGMP Snooping Status per Interface" on page 386).

When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.

■ **Proxy Reporting Status** – Enables IGMP Snooping with Proxy Reporting. (Default: Disabled)

When proxy reporting is enabled with this command, the switch performs "IGMP Snooping with Proxy Reporting" (as defined in DSL Forum TR-101, April 2006), including last leave, and query suppression.

Last leave sends out a proxy query when the last member leaves a multicast group, and query suppression means that neither specific queries nor general queries are forwarded from an upstream multicast router to hosts downstream from this device.

- **TCN Flood** – Enables flooding of multicast traffic if a spanning tree topology change notification (TCN) occurs. (Default: Disabled)

  When a spanning tree topology change occurs, the multicast membership information learned by switch may be out of date. For example, a host linked to one port before the topology change (TC) may be moved to another port after the change. To ensure that multicast data is delivered to all receivers, by default, a switch in a VLAN (with IGMP snooping enabled) that receives a Bridge Protocol Data Unit (BPDU) with TC bit set (by the root bridge) will enter into "multicast flooding mode" for a period of time until the topology has stabilized and the new locations of all multicast receivers are learned.

  If a topology change notification (TCN) is received, and all the uplink ports are subsequently deleted, a time out mechanism is used to delete all of the currently learned multicast channels.

  When a new uplink port starts up, the switch sends unsolicited reports for all currently learned channels out the new uplink port.

  By default, the switch immediately enters into "multicast flooding mode" when a spanning tree topology change occurs. In this mode, multicast traffic will be flooded to all VLAN ports. If many ports have subscribed to different multicast groups, flooding may cause excessive packet loss on the link between the switch and the end host. Flooding may be disabled to avoid this, causing multicast traffic to be delivered only to those ports on which multicast group members have been learned. Otherwise, the time spent in flooding mode can be manually configured to reduce excessive loading.

  When the spanning tree topology changes, the root bridge sends a proxy query to quickly re-learn the host membership/port relations for multicast channels. The root bridge also sends an unsolicited Multicast Router Discover (MRD) request to quickly locate the multicast routers in this VLAN.

  The proxy query and unsolicited MRD request are flooded to all VLAN ports except for the receiving port when the switch receives such packets.

- **TCN Query Solicit** – Sends out an IGMP general query solicitation when a spanning tree topology change notification (TCN) occurs. (Default: Disabled)

  When the root bridge in a spanning tree receives a TCN for a VLAN where IGMP snooping is enabled, it issues a global IGMP leave message (or query solicitation). When a switch receives this solicitation, it floods it to all ports in the VLAN where the spanning tree change occurred. When an upstream multicast router receives this solicitation, it immediately issues an IGMP general query.

  A query solicitation can be sent whenever the switch notices a topology change, even if it is not the root bridge in spanning tree.

- **Router Alert Option** – Discards any IGMPv2/v3 packets that do not include the Router Alert option. (Default: Disabled)

As described in Section 9.1 of RFC 3376 for IGMP Version 3, the Router Alert Option can be used to protect against DOS attacks. One common method of attack is launched by an intruder who takes over the role of querier, and starts overloading multicast hosts by sending a large number of group-and-source-specific queries, each with a large source list and the Maximum Response Time set to a large value.

To protect against this kind of attack, (1) routers should not forward queries. This is easier to accomplish if the query carries the Router Alert option. (2) Also, when the switch is acting in the role of a multicast host (such as when using proxy routing), it should ignore version 2 or 3 queries that do not contain the Router Alert option.

- **Unregistered Data Flooding** – Floods unregistered multicast traffic into the attached VLAN. (Default: Disabled)

  Once the table used to store multicast entries for IGMP snooping and multicast routing is filled, no new entries are learned. If no router port is configured in the attached VLAN, and unregistered-flooding is disabled, any subsequent multicast traffic not found in the table is dropped, otherwise it is flooded throughout the VLAN.

- **Version Exclusive** – Discards any received IGMP messages which use a version different to that currently configured by the IGMP Version attribute. (Default: Disabled)

- **IGMP Unsolicited Report Interval** – Specifies how often the upstream interface should transmit unsolicited IGMP reports when proxy reporting is enabled. (Range: 1-65535 seconds, Default: 400 seconds)

  When a new upstream interface (that is, uplink port) starts up, the switch sends unsolicited reports for all currently learned multicast channels via the new upstream interface.

  This command only applies when proxy reporting is enabled.

- **Router Port Expire Time** – The time the switch waits after the previous querier stops before it considers it to have expired. (Range: 1-65535, Recommended Range: 300-500 seconds, Default: 300)

- **IGMP Snooping Version** – Sets the protocol version for compatibility with other devices on the network. This is the IGMP Version the switch uses to send snooping reports. (Range: 1-3; Default: 2)

  This attribute configures the IGMP report/query version used by IGMP snooping. Versions 1 - 3 are all supported, and versions 2 and 3 are backward compatible, so the switch can operate with other devices, regardless of the snooping version employed.

- **Querier Status** – When enabled, the switch can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic. This feature is not supported for IGMPv3 snooping. (Default: Disabled)

#### WEB INTERFACE

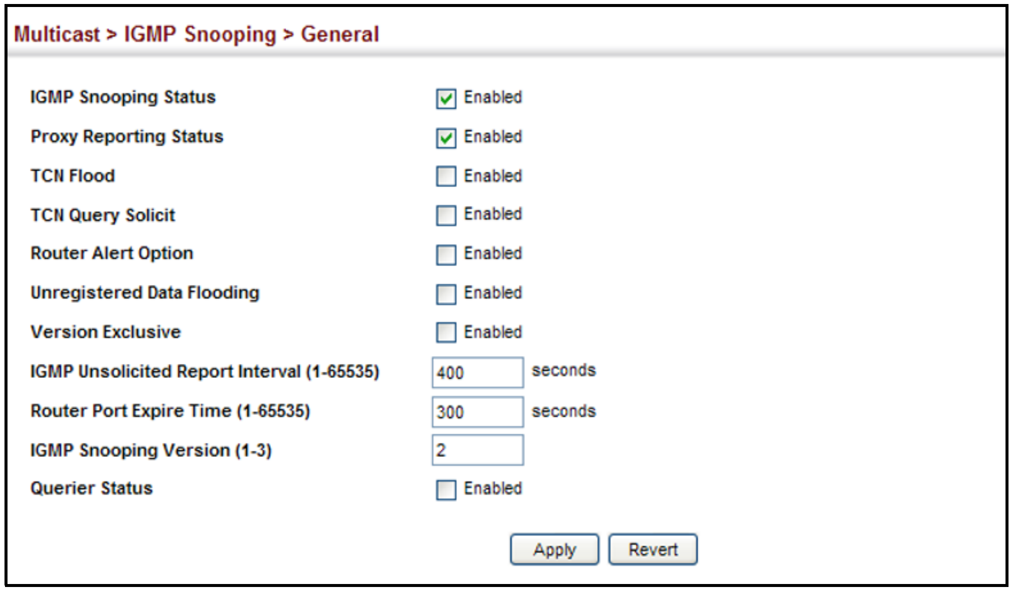
To configure general settings for IGMP Snooping and Query:

1. Click Multicast, IGMP Snooping, General.

2. Adjust the IGMP settings as required.

3. Click Apply.

**Figure 3: Configuring General Settings for IGMP Snooping**




## Specifying Static Interfaces for a Multicast Router

Use the Multicast > IGMP Snooping > Multicast Router (Add Static Multicast Router) page to statically attach an interface to a multicast router/switch.

Depending on network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on the switch, the interface (and a specified VLAN) can be manually configured to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the switch.

### CLI REFERENCES

- "Static Multicast Routing" on page 974

### PARAMETERS

These parameters are displayed in the web interface:

- **VLAN** – Selects the VLAN which is to propagate all multicast traffic coming from the attached multicast router. (Range: 1-4093)

- **Interface** – Activates the Port or Trunk scroll down list.

- **Port** or **Trunk** – Specifies the interface attached to a multicast router.

### WEB INTERFACE

To specify a static interface attached to a multicast router:

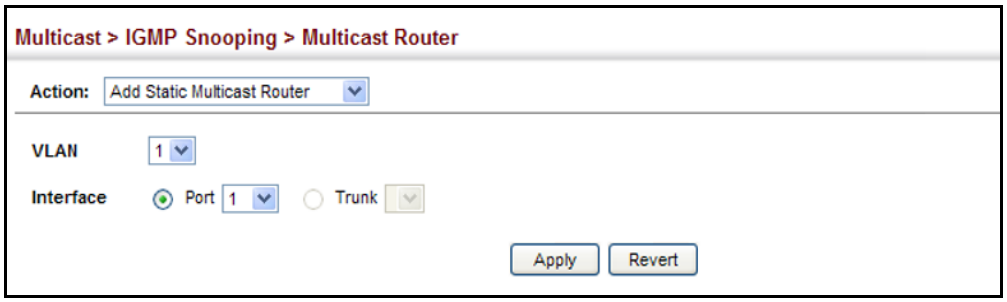
1. Click Multicast, IGMP Snooping, Multicast Router.

2. Select Add Static Multicast Router from the Action list.

3. Select the VLAN which will forward all the corresponding multicast traffic, and select the port or trunk attached to the multicast router.

4. Click Apply.

**Figure 4: Configuring a Static Interface for a Multicast Router**



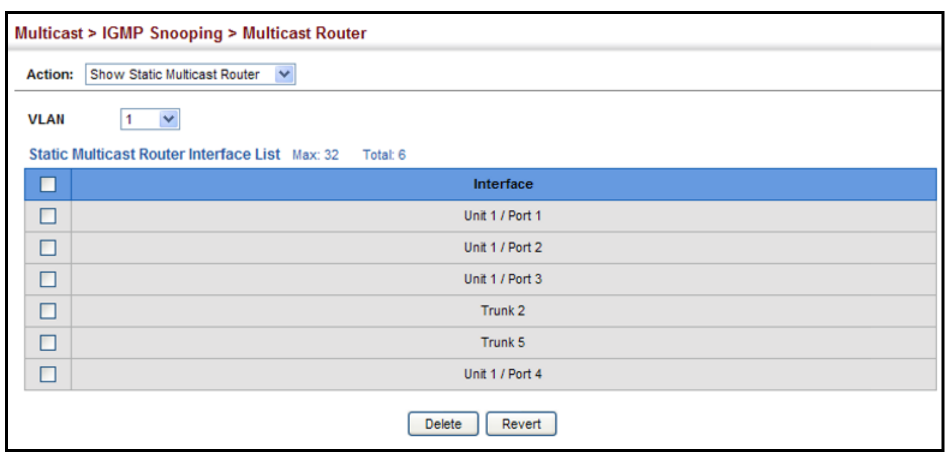

To show the static interfaces attached to a multicast router:

1. Click Multicast, IGMP Snooping, Multicast Router.

2. Select Show Static Multicast Router from the Action list.

3. Select the VLAN for which to display this information.

**Figure 5: Showing Static Interfaces Attached a Multicast Router**



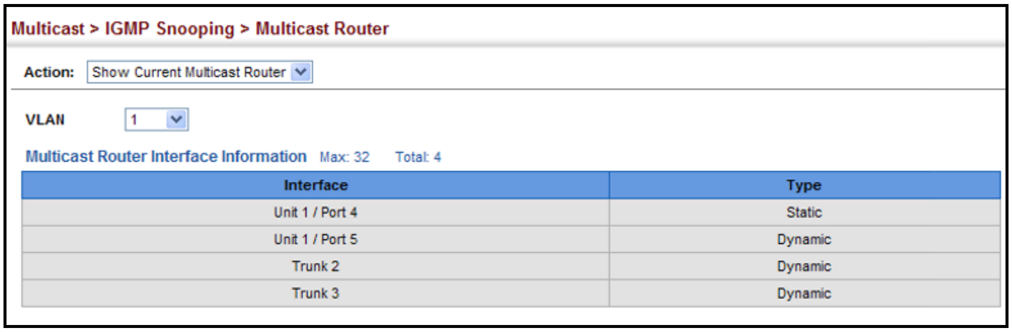

Multicast routers that are attached to ports on the switch use information obtained from IGMP, along with a multicast routing protocol (such as PIM) to support IP multicasting across the Internet. These routers may be dynamically discovered by the switch or statically assigned to an interface on the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

1. Click Multicast, IGMP Snooping, Multicast Router.

2. Select Current Multicast Router from the Action list.

3. Select the VLAN for which to display this information. Ports in the selected VLAN which are attached to a neighboring multicast router/switch are displayed.

**Figure 6: Showing Current Interfaces Attached a Multicast Router**




## Assigning Interfaces to Multicast Services

Use the Multicast > IGMP Snooping > IGMP Member (Add Static Member) page to statically assign a multicast service to an interface.

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages (see "Configuring IGMP Snooping and Query Parameters" on page 379). However, for certain applications that require tighter control, it may be necessary to statically configure a multicast service on the switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

### CLI REFERENCES

■ "ip igmp snooping vlan static" on page 971

### COMMAND USAGE

■ Static multicast addresses are never aged out.

■ When a multicast address is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

### PARAMETERS

These parameters are displayed in the web interface:

■ **VLAN** – Specifies the VLAN which is to propagate the multicast service. (Range: 1-4093)

■ **Interface** – Activates the Port or Trunk scroll down list.

■ **Port** or **Trunk** – Specifies the interface assigned to a multicast group.

■ **Multicast IP** – The IP address for a specific multicast service.

### WEB INTERFACE

To statically assign an interface to a multicast service:

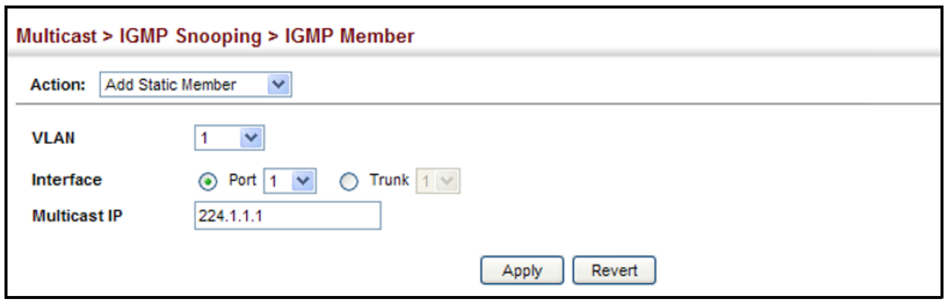
1. Click Multicast, IGMP Snooping, IGMP Member.

2. Select Add Static Member from the Action list.

3. Select the VLAN that will propagate the multicast service, specify the interface attached to a multicast service (through an IGMP-enabled switch or multicast router), and enter the multicast IP address.

4. Click Apply.

**Figure 7: Assigning an Interface to a Multicast Service**



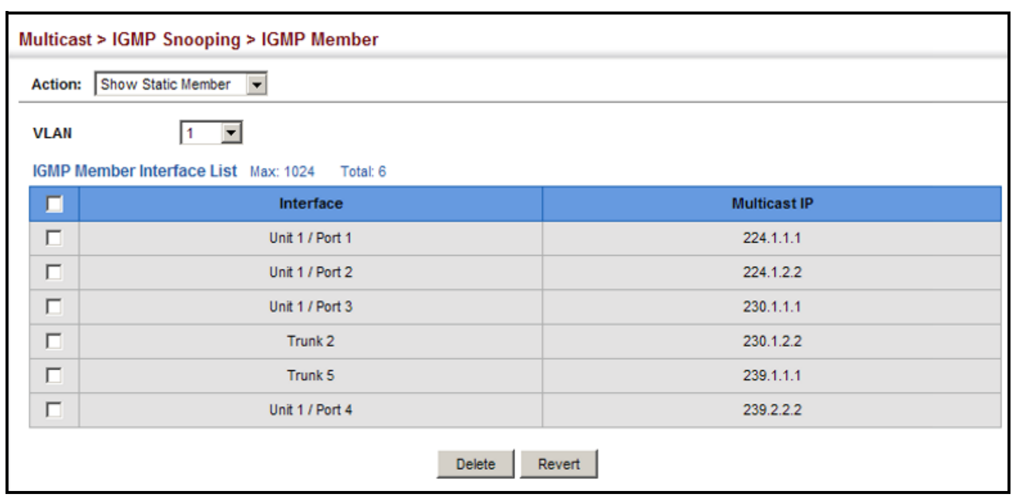

To show the static interfaces assigned to a multicast service:

1. Click Multicast, IGMP Snooping, IGMP Member.

2. Select Show Static Member from the Action list.

3. Select the VLAN for which to display this information.

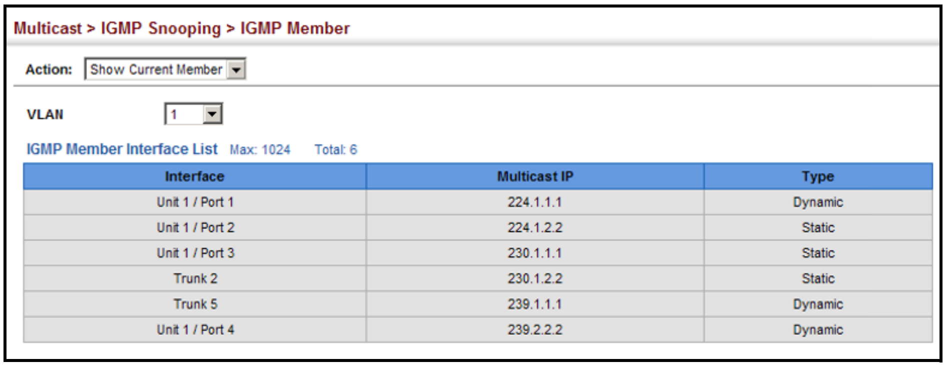
**Figure 8: Showing Static Interfaces Assigned to a Multicast Service**



To display information about all multicast groups, IGMP Snooping or multicast routing must first be enabled on the switch. To show all of the interfaces statically or dynamically assigned to a multicast service:

1. Click Multicast, IGMP Snooping, IGMP Member.
2. Select Show Current Member from the Action list.
3. Select the VLAN for which to display this information.

**Figure 9: Showing Current Interfaces Assigned to a Multicast Service**




| Interface | Multicast IP | Type |
|---|---|---|
| Unit 1 / Port 1 | 224.1.1.1 | Dynamic |
| Unit 1 / Port 2 | 224.1.2.2 | Static |
| Unit 1 / Port 3 | 230.1.1.1 | Static |
| Trunk 2 | 230.1.2.2 | Static |
| Trunk 5 | 239.1.1.1 | Dynamic |
| Unit 1 / Port 4 | 239.2.2.2 | Dynamic |

## Setting IGMP Snooping Status per Interface

Use the Multicast > IGMP Snooping > Interface (Configure VLAN) page to configure IGMP snooping attributes for a VLAN interface. To configure snooping globally, refer to "Configuring IGMP Snooping and Query Parameters" on page 379.

### CLI REFERENCES

- "IGMP Snooping" on page 957

### COMMAND USAGE

*Multicast Router Discovery*

There have been many mechanisms used in the past to identify multicast routers. This has lead to interoperability issues between multicast routers and snooping switches from different vendors. In response to this problem, the Multicast Router Discovery (MRD) protocol has been developed for use by IGMP snooping and multicast routing devices. MRD is used to discover which interfaces are attached to multicast routers, allowing IGMP-enabled devices to determine where to send multicast source and group membership messages. (MRD is specified in draft-ietf-magma-mrdisc-07.)

Multicast source data and group membership reports must be received by all multicast routers on a segment. Using the group membership protocol query messages to discover multicast routers is insufficient due to query suppression. MRD therefore provides a standardized way to identify multicast routers without relying on any particular multicast routing protocol.

**NOTE:** The default values recommended in the MRD draft are implemented in the switch.

Multicast Router Discovery uses the following three message types to discover multicast routers:

- Multicast Router Advertisement – Advertisements are sent by routers to advertise that IP multicast forwarding is enabled. These messages are sent unsolicited periodically on all router interfaces on which multicast forwarding is enabled. They are sent upon the occurrence of these events:
  - Upon the expiration of a periodic (randomized) timer.
  - As a part of a router's start up procedure.
  - During the restart of a multicast forwarding interface.
  - On receipt of a Solicitation message.
- Multicast Router Solicitation – Devices send Solicitation messages in order to solicit Advertisement messages from multicast routers. These messages are used to discover multicast routers on a directly attached link. Solicitation messages are also sent whenever a multicast forwarding interface is initialized or re-initialized. Upon receiving a solicitation on an interface with IP multicast forwarding and MRD enabled, a router will respond with an Advertisement.
- Multicast Router Termination – These messages are sent when a router stops IP multicast routing functions on an interface. Termination messages are sent by multicast routers when:
  - Multicast forwarding is disabled on an interface.
  - An interface is administratively disabled.
  - The router is gracefully shut down.

Advertisement and Termination messages are sent to the All-Snoopers multicast address. Solicitation messages are sent to the All-Routers multicast address.

**NOTE:** MRD messages are flooded to all ports in a VLAN where IGMP snooping or routing has been enabled. To ensure that older switches which do not support MRD can also learn the multicast router port, the switch floods IGMP general query packets, which do not have a null source address (0.0.0.0), to all ports in the attached VLAN. IGMP packets with a null source address are only flooded to all ports in the VLAN if the system is operating in multicast flooding mode, such as when a new VLAN or new router port is being established, or an spanning tree topology change has occurred. Otherwise, this kind of packet is only forwarded to known multicast routing ports.

### PARAMETERS

These parameters are displayed in the web interface:

- **VLAN** – ID of configured VLANs. (Range: 1-4093)
- **IGMP Snooping Status** – When enabled, the switch will monitor network traffic on the indicated VLAN interface to determine which hosts want to receive multicast traffic. This is referred to as IGMP Snooping. (Default: Disabled)

  When IGMP snooping is enabled globally (see page 379), the per VLAN interface settings for IGMP snooping take precedence.

When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.

- **Version Exclusive** – Discards any received IGMP messages (except for multicast protocol packets) which use a version different to that currently configured by the IGMP Version attribute. (Default: Disabled)

  If version exclusive is disabled on a VLAN, then this setting is based on the global setting configured on the Multicast > IGMP Snooping > General page. If it is enabled on a VLAN, then this setting takes precedence over the global setting.

- **Immediate Leave Status** – Immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate leave is enabled for the parent VLAN. (Default: Disabled)

  If immediate leave is not used, a multicast router (or querier) will send a group-specific query message when an IGMPv2 group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the specified time out period. Note that this time out is defined by Last Member Query Interval * Robustness Variable (fixed at 2 as defined in RFC 2236).

  If immediate leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one IGMP-enabled device, either a service host or a neighbor running IGMP snooping.

  This attribute is only effective if IGMP snooping is enabled, and IGMPv2 snooping is used.

- **Multicast Router Discovery** – MRD is used to discover which interfaces are attached to multicast routers. (Default: Enabled)

- **General Query Suppression** – Suppresses general queries except for ports attached to downstream multicast hosts. (Default: Disabled)

  By default, general query messages are flooded to all ports, except for the multicast router through which they are received.

  If general query suppression is enabled, then these messages are forwarded only to downstream ports which have joined a multicast service.

- **Proxy Reporting** – Enables IGMP Snooping with Proxy Reporting. (Default: Based on global setting)

  When proxy reporting is enabled with this command, the switch performs “IGMP Snooping with Proxy Reporting” (as defined in DSL Forum TR-101, April 2006), including last leave, and query suppression.

  Last leave sends out a proxy query when the last member leaves a multicast group, and query suppression means that neither specific queries nor general queries are forwarded from an upstream multicast router to hosts downstream from this device.

  If proxy reporting is disabled, report suppression can still be configured by a separate attribute as described above.

- **Interface Version** – Sets the protocol version for compatibility with other devices on the network. This is the IGMP Version the switch uses to send snooping reports. (Range: 1-3; Default: 2)

  This attribute configures the IGMP report/query version used by IGMP snooping. Versions 1 - 3 are all supported, and versions 2 and 3 are backward compatible, so the switch can operate with other devices, regardless of the snooping version employed.

- **Query Interval** – The interval between sending IGMP proxy general queries. (Range: 2-31744 seconds; Default: 125 seconds)

  An IGMP general query message is sent by the switch at the interval specified by this attribute. When this message is received by downstream hosts, all receivers build an IGMP report for the multicast groups they have joined.

  This attribute applies when the switch is serving as the querier (page 379), or as a proxy host when IGMP snooping proxy reporting is enabled (page 379).

- **Query Response Interval** – The maximum time the system waits for a response to proxy general queries. (Range: 10-31744 tenths of a second; Default: 10 seconds)

  This attribute applies when the switch is serving as the querier (page 379), or as a proxy host when IGMP snooping proxy reporting is enabled (page 379).

- **Last Member Query Interval** – The interval to wait for a response to a group-specific or group-and-source-specific query message. (Range: 1-31744 tenths of a second in multiples of 10;
  Default: 1 second)

  When a multicast host leaves a group, it sends an IGMP leave message. When the leave message is received by the switch, it checks to see if this host is the last to leave the group by sending out an IGMP group-specific or group-and-source-specific query message, and starts a timer. If no reports are received before the timer expires, the group record is deleted, and a report is sent to the upstream multicast router.

  A reduced value will result in reduced time to detect the loss of the last member of a group or source, but may generate more burst traffic.

  This attribute will take effect only if IGMP snooping proxy reporting is enabled (see page 379).

- **Last Member Query Count** – The number of IGMP proxy group-specific or group-and-source-specific query messages that are sent out before the system assumes there are no more local members. (Range: 1-255; Default: 2)

  This attribute will take effect only if IGMP snooping proxy reporting or IGMP querier is enabled.

- **Proxy Query Address** – A static source address for locally generated query and report messages used by IGMP Proxy Reporting. (Range: Any valid IP unicast address; Default: 0.0.0.0)

  IGMP Snooping uses a null IP address of 0.0.0.0 for the source of IGMP query messages which are proxied to downstream hosts to indicate that it is not the elected querier, but is only proxying these messages as defined in RFC 4541. The switch also uses a null address in IGMP reports sent to upstream ports.

Many hosts do not implement RFC 4541, and therefore do not understand query messages with the source address of 0.0.0.0. These hosts will therefore not reply to the queries, causing the multicast router to stop sending traffic to them.

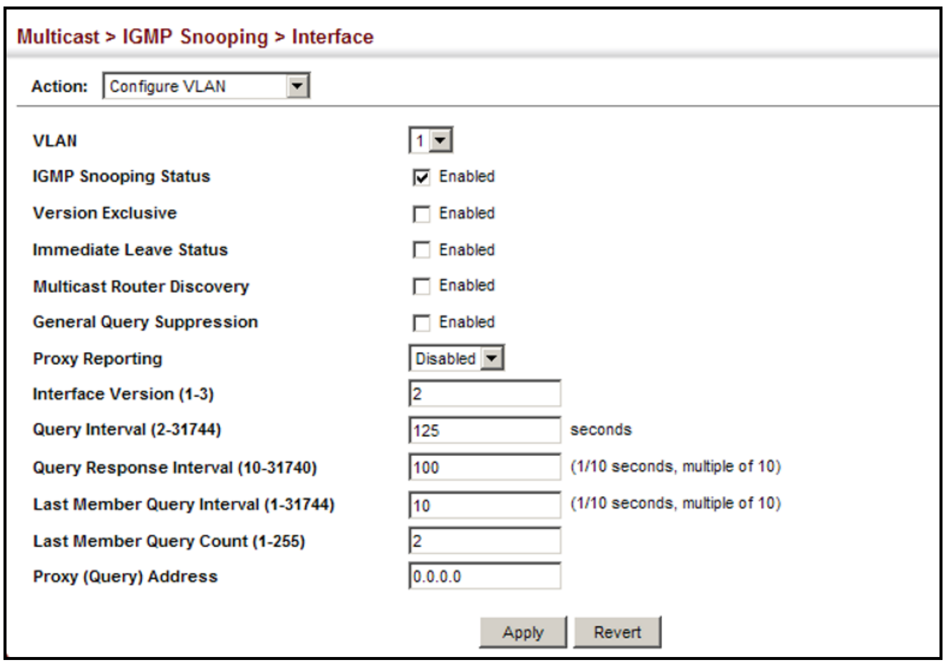
To resolve this problem, the source address in proxied IGMP query messages can be replaced with any valid unicast address (other than the router's own address).

### WEB INTERFACE

To configure IGMP snooping on a VLAN:

1. Click Multicast, IGMP Snooping, Interface.
2. Select Configure VLAN from the Action list.
3. Select the VLAN to configure and update the required parameters.
4. Click Apply.

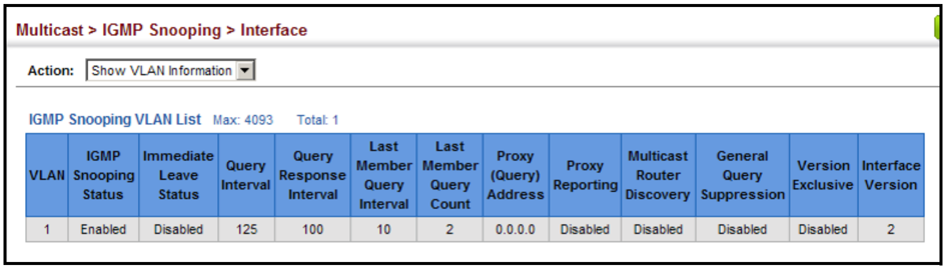
**Figure 10: Configuring IGMP Snooping on an Interface**




To show the interface settings for IGMP snooping:

1. Click Multicast, IGMP Snooping, Interface.
2. Select Show VLAN Information from the Action list.

**Figure 11: Showing Interface Settings for IGMP Snooping**




## Filtering IGMP Query Packets and Multicast Data

Use the Multicast > IGMP Snooping > Interface (Configure Port/Trunk) page to configure an interface to drop IGMP query packets or multicast data packets.

### CLI REFERENCES

- "ip igmp query-drop" on page 980
- "ip multicast-data-drop" on page 981

### PARAMETERS

These parameters are displayed in the web interface:

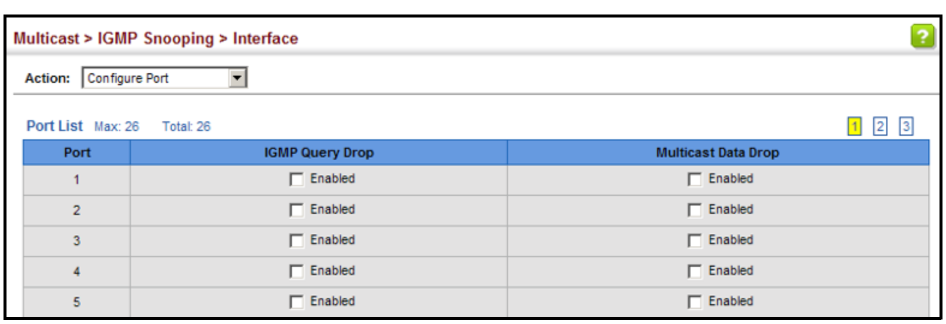
- **IGMP Query Drop** – Configures an interface to drop any IGMP query packets received on the specified interface. If this switch is acting as a Querier, this prevents it from being affected by messages received from another Querier.
- **Multicast Data Drop** – Configures an interface to stop multicast services from being forwarded to users attached to the downstream port (i.e., the interfaces specified by this command).

### WEB INTERFACE

To drop IGMP query packets or multicast data packets:

1. Click Multicast, IGMP Snooping, Interface.
2. Select Configure Port or Configure Trunk from the Action List.
3. Enable the required drop functions for any interface.
4. Click Apply.

**Figure 12: Dropping IGMP Query or Multicast Data Packets**



## Displaying Multicast Groups Discovered by IGMP Snooping

Use the Multicast > IGMP Snooping > Forwarding Entry page to display the forwarding entries learned through IGMP Snooping.

**CLI REFERENCES**

- "show ip igmp snooping group" on page 973

**COMMAND USAGE**

To display information about multicast groups, IGMP Snooping must first be enabled on the switch (see page 379).

**PARAMETERS**

These parameters are displayed in the web interface:

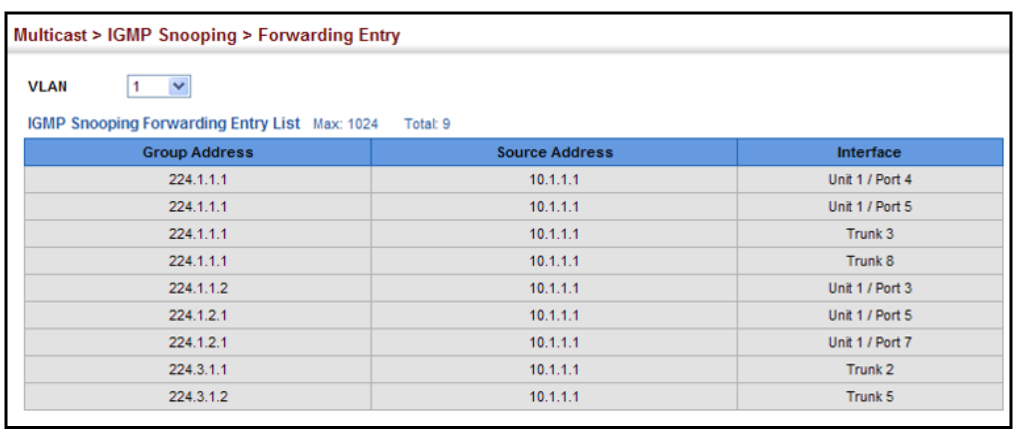
- **VLAN** – An interface on the switch that is forwarding traffic to downstream ports for the specified multicast group address.
- **Group Address** – IP multicast group address with subscribers directly attached or downstream from the switch, or a static multicast group assigned to this interface.
- **Source Address** – The address of one of the multicast servers transmitting traffic to the specified group.
- **Interface** – A downstream port or trunk that is receiving traffic for the specified multicast group. This field may include both dynamically and statically configured multicast router ports.

**WEB INTERFACE**

To show multicast groups learned through IGMP snooping:

1. Click Multicast, IGMP Snooping, Forwarding Entry.
2. Select the VLAN for which to display this information.

**Figure 13: Showing Multicast Groups Learned by IGMP Snooping**




| Group Address | Source Address | Interface |
|---|---|---|
| 224.1.1.1 | 10.1.1.1 | Unit 1 / Port 4 |
| 224.1.1.1 | 10.1.1.1 | Unit 1 / Port 5 |
| 224.1.1.1 | 10.1.1.1 | Trunk 3 |
| 224.1.1.1 | 10.1.1.1 | Trunk 8 |
| 224.1.1.2 | 10.1.1.1 | Unit 1 / Port 3 |
| 224.1.2.1 | 10.1.1.1 | Unit 1 / Port 5 |
| 224.1.2.1 | 10.1.1.1 | Unit 1 / Port 7 |
| 224.3.1.1 | 10.1.1.1 | Trunk 2 |
| 224.3.1.2 | 10.1.1.1 | Trunk 5 |

# FILTERING AND THROTTLING IGMP GROUPS

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The IGMP filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and IGMP throttling limits the number of simultaneous multicast groups a port can join.

IGMP filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. An IGMP filter profile can contain one or more addresses, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, IGMP join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the IGMP join report is forwarded as normal. If a requested multicast group is denied, the IGMP join report is dropped.

IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

## Enabling IGMP Filtering and Throttling

Use the Multicast > IGMP Snooping > Filter (Configure General) page to enable IGMP filtering and throttling globally on the switch.

### CLI REFERENCES

- "ip igmp filter (Global Configuration)" on page 976

### PARAMETERS

These parameters are displayed in the web interface:

- **IGMP Filter Status** – Enables IGMP filtering and throttling globally for the switch. (Default: Disabled)

### WEB INTERFACE

To enables IGMP filtering and throttling on the switch:

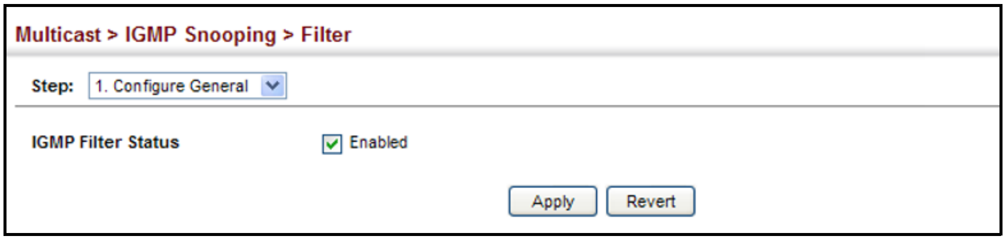
1. Click Multicast, IGMP Snooping, Filtering.

2. Select Configure General from the Action list.

3. Enable IGMP Filter Status.

4. Click Apply.

**Figure 14: Enabling IGMP Filtering and Throttling**




## Configuring IGMP Filter Profiles

Use the Multicast > IGMP Snooping > Filter (Add) page to create an IGMP profile and set its access mode. Then use the (Add Multicast Group Range) page to configure the multicast groups to filter.

### CLI REFERENCES

- "IGMP Filtering and Throttling" on page 975

### COMMAND USAGE

Specify a range of multicast groups by entering a start and end IP address; or specify a single multicast group by entering the same IP address for the start and end of the range.

### PARAMETERS

These parameters are displayed in the web interface:

*Add*

- **Profile ID** – Creates an IGMP profile. (Range: 1-4294967295)

- **Access Mode** – Sets the access mode of the profile; either permit or deny. (Default: Deny)

  When the access mode is set to permit, IGMP join reports are processed when a multicast group falls within the controlled range. When the access mode is set to deny, IGMP join reports are only processed when the multicast group is not in the controlled range.

*Add Multicast Group Range*

- **Profile ID** – Selects an IGMP profile to configure.

- **Start Multicast IP Address** – Specifies the starting address of a range of multicast groups.

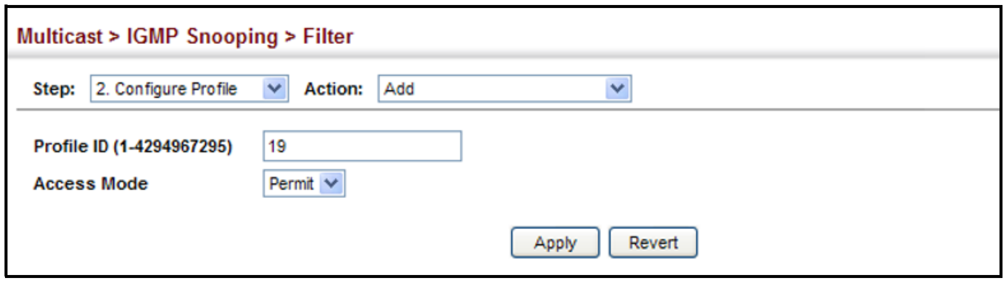
- **End Multicast IP Address** – Specifies the ending address of a range of multicast groups.

### WEB INTERFACE

To create an IGMP filter profile and set its access mode:

1. Click Multicast, IGMP Snooping, Filtering.
2. Select Add from the Action list.
3. Enter the number for a profile, and set its access mode.
4. Click Apply.

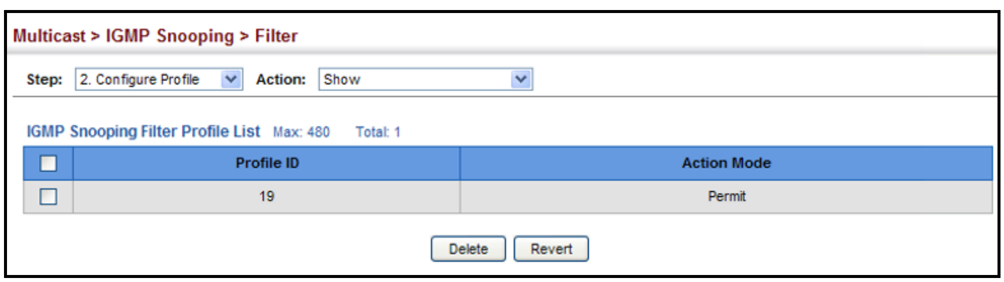
**Figure 15: Creating an IGMP Filtering Profile**




To show the IGMP filter profiles:

1. Click Multicast, IGMP Snooping, Filtering.
2. Select Show from the Action list.

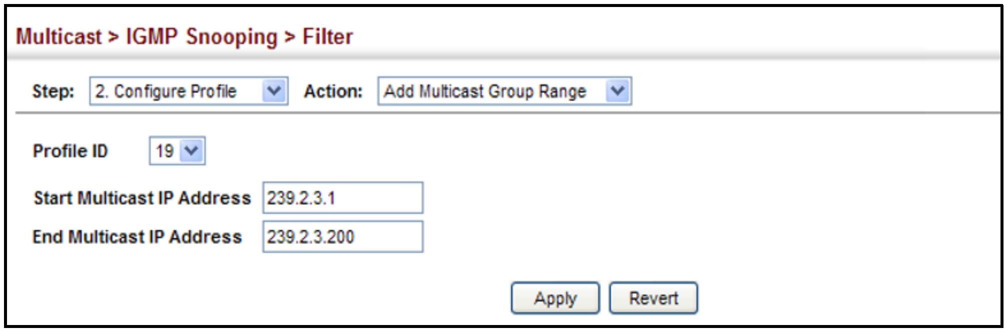
**Figure 16: Showing the IGMP Filtering Profiles Created**




To add a range of multicast groups to an IGMP filter profile:

1. Click Multicast, IGMP Snooping, Filtering.
2. Select Add Multicast Group Range from the Action list.
3. Select the profile to configure, and add a multicast group address or range of addresses.
4. Click Apply.

**Figure 17: Adding Multicast Groups to an IGMP Filtering Profile**



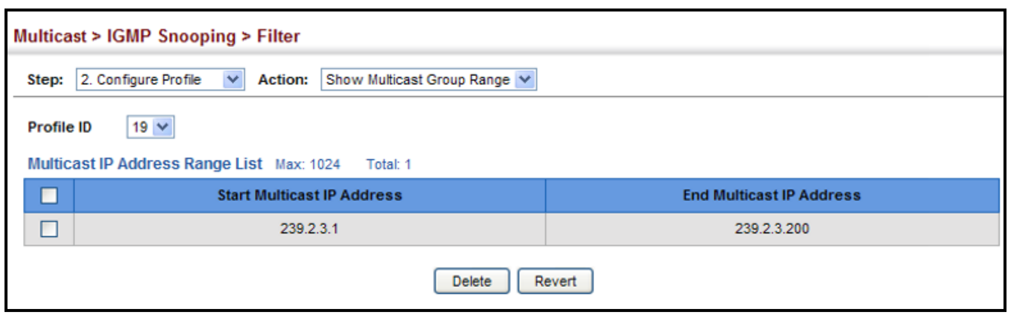

To show the multicast groups configured for an IGMP filter profile:

**1.** Click Multicast, IGMP Snooping, Filtering.

**2.** Select Show Multicast Group Range from the Action list.

**3.** Select the profile for which to display this information.

**Figure 18: Showing the Groups Assigned to an IGMP Filtering Profile**




## Configuring IGMP Filtering and Throttling for Interfaces

Use the Multicast > IGMP Snooping > Configure Interface page to assign and IGMP filter profile to interfaces on the switch, or to throttle multicast traffic by limiting the maximum number of multicast groups an interface can join at the same time.

### CLI REFERENCES

■"IGMP Filtering and Throttling" on page 975

### COMMAND USAGE

■IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

### PARAMETERS

These parameters are displayed in the web interface:

■**Interface** – Port or trunk identifier.

An IGMP profile or throttling setting can be applied to a port or trunk. When ports are configured as trunk members, the trunk uses the settings applied to the first port member in the trunk.

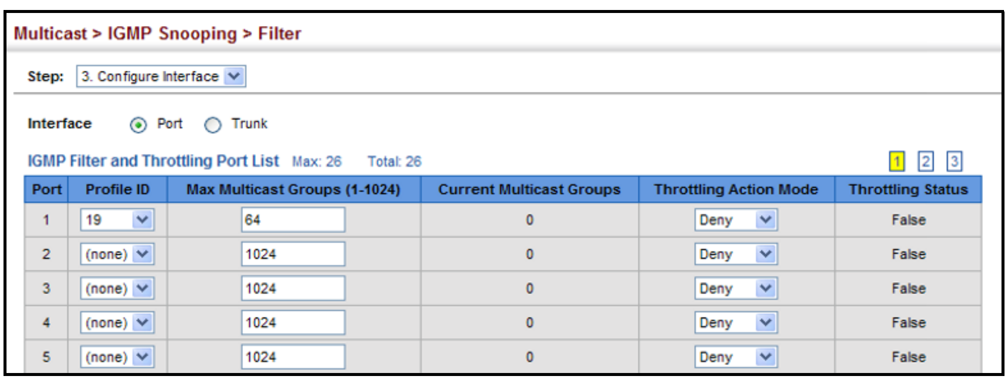
- **Profile ID** – Selects an existing profile to assign to an interface.
- **Max Multicast Groups** – Sets the maximum number of multicast groups an interface can join at the same time. (Range: 1-1024; Default: 1024)
- **Current Multicast Groups** – Displays the current multicast groups the interface has joined.
- **Throttling Action Mode** – Sets the action to take when the maximum number of multicast groups for the interface has been exceeded. (Default: Deny)
  - **Deny** - The new multicast group join report is dropped.
  - **Replace** - The new multicast group replaces an existing group.
- **Throttling Status** – Indicates if the throttling action has been implemented on the interface. (Options: True or False)

### WEB INTERFACE

To configure IGMP filtering or throttling for a port or trunk:

1. Click Multicast, IGMP Snooping, Filtering.
2. Select Configure Interface from the Action list.
3. Select a profile to assign to an interface, then set the maximum number of allowed multicast groups and the throttling response.
4. Click Apply.

**Figure 19: Configuring IGMP Filtering and Throttling Interface Settings**




| Port | Profile ID | Max Multicast Groups (1-1024) | Current Multicast Groups | Throttling Action Mode | Throttling Status |
|---|---|---|---|---|---|
| 1 | 19 | 64 | 0 | Deny | False |
| 2 | (none) | 1024 | 0 | Deny | False |
| 3 | (none) | 1024 | 0 | Deny | False |
| 4 | (none) | 1024 | 0 | Deny | False |
| 5 | (none) | 1024 | 0 | Deny | False |

## LAYER 3 IGMP (QUERY USED WITH MULTICAST ROUTING)

IGMP Snooping – IGMP Snooping (page 379) is a key part of the overall set of functions required to support multicast filtering. It is used to passively monitor IGMP service requests from multicast clients, and dynamically configure the switch ports which need to forward multicast traffic.

IGMP Query – Multicast query is used to poll each known multicast group for active members, and dynamically configure the switch ports which need to forward multicast traffic. Layer 3 IGMP Query, as described below, is used in conjunction with both Layer 2 IGMP Snooping and multicast routing.

IGMP – This protocol includes a form of multicast query specifically designed to work with multicast routing. A router periodically asks its hosts if they want to receive multicast traffic. It then propagates service requests on to any upstream multicast router to ensure that it will continue to receive the multicast service. IGMP can be enabled for individual VLAN interfaces (page 401).

**NOTE:** Multicast Routing Discovery (MRD) is used to discover which interfaces are attached to multicast routers. (For a description of this protocol, see “Multicast Router Discovery” on page 386.)

IGMP Proxy – A device can learn about the multicast service requirements of hosts attached to its downstream interfaces, proxy this group membership information to the upstream router, and forward multicast packets based on that information.

## Configuring IGMP Proxy Routing

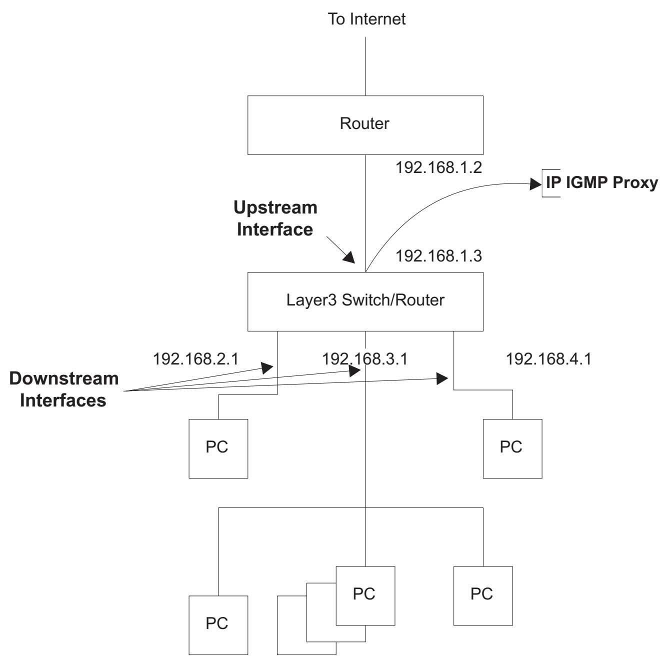
Use the Multicast > IGMP > Proxy page to configure IGMP Proxy Routing.

In simple network topologies, it is sufficient for a device to learn multicast requirements from its downstream interfaces and proxy this group membership information to the upstream router. Multicast packets can then be forwarded downstream based solely upon that information. This mechanism, known as IGMP proxy routing, enables the system to issue IGMP host messages on behalf of hosts that the system has discovered through standard IGMP interfaces.

### CLI REFERENCES

■"IGMP Proxy Routing" on page 1000

**Figure 20: IGMP Proxy Routing**




Using IGMP proxy routing to forward multicast traffic on edge switches greatly reduces the processing load on those devices by not having to run more complicated multicast routing protocols such as PIM. It also makes the proxy devices independent of the multicast routing protocols used by core routers.

IGMP proxy routing uses a tree topology, where the root of the tree is connected to a complete multicast infrastructure (with the upstream interface connected to the Internet as shown in the figure above). In such a simple topology, it is sufficient to send the group membership information learned upstream, and then to forward multicast packets based upon that information to the downstream hosts. For the switch, IGMP proxy routing has only one upstream connection to the core network side and multiple downstream connections to the customer side.

The IGMP proxy routing tree must be manually configured by designating one upstream interface and multiple downstream interfaces on each proxy device. No other multicast routers except for the proxy devices can exist within the tree, and the root of the tree must be connected to a wider multicast infrastructure. Note that this protocol is limited to a single administrative domain.

In more complicated scenarios where the topology is not a tree (such as when there are diverse paths to multiple sources), a more robust failover mechanism should be used. If more than one administrative domain is involved, a multicast routing protocol should be used instead of IGMP proxy.

To enable IGMP proxy service, follow these steps:

1. Enable IP multicasting globally on the router (see "Configuring Global Settings for Multicast Routing" on page 568).

2. Enable IGMP on the downstream interfaces which require proxy multicast service (see "Configuring IGMP Interface Parameters" on page 401).

3. Enable IGMP proxy on the interface that is attached to an upstream multicast router using the proxy settings described in this section.

4. Optional – Indicate how often the system will send unsolicited reports to the upstream router using the Multicast > IGMP > Proxy page as described later in this section.

### COMMAND USAGE

- When IGMP proxy is enabled on an interface, that interface is known as the upstream or host interface. This interface performs only the host portion of IGMP by sending IGMP membership reports, and automatically disables IGMP router functions.

- Interfaces with IGMP enabled, but not located in the direction of the multicast tree root are known as downstream or router interfaces. These interfaces perform the standard IGMP router functions by maintaining a database of all IGMP subscriptions on the downstream interface. IGMP must therefore be enabled on all interfaces which require proxy multicast service.

- The system periodically checks the multicast route table for (*,G) any-source multicast forwarding entries. When changes occur in the downstream IGMP groups, an IGMP state change report is created and sent to the upstream router.

- If there is an IGMPv1 or IGMPv2 querier on the upstream network, then the proxy device will act as an IGMPv1 or IGMPv2 host on the upstream interface accordingly, and set the v1/v2 query present timer to indicate that there is an active v1/v2 querier in this VLAN. Otherwise, it will act as an IGMPv3 host.

- Multicast routing protocols are not supported when IGMP proxy service is enabled.

- Only one upstream interface is supported on the system.

- A maximum of 1024 multicast entries are supported.

### PARAMETERS

These parameters are displayed in the web interface:

- **VLAN** – VLAN interface on which to configure IGMP proxy service. (Range: 1-4093)

- **IGMP Proxy Status** – Enables IGMP proxy service for multicast routing, forwarding IGMP membership information monitored on downstream interfaces onto the upstream interface in a summarized report. (Default: Disabled)

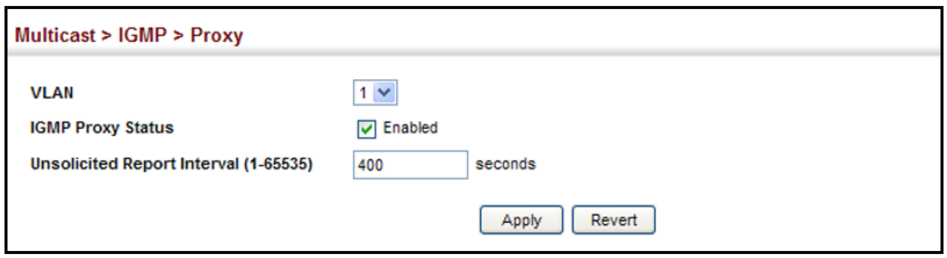
- **Unsolicited Report Interval** – Specifies how often the upstream interface should transmit unsolicited IGMP reports. (Range: 1-65535 seconds; Default: 400 seconds)

**WEB INTERFACE**

To configure IGMP Proxy Routing:

1. Click Multicast, IGMP, Proxy.
2. Select the upstream interface, enable the IGMP Proxy Status, and modify the interval for unsolicited IGMP reports if required.
3. Click Apply.

**Figure 21: Configuring IGMP Proxy Routing**




## Configuring IGMP Interface Parameters

Use the Multicast > IGMP > Interface page to configure interface settings for IGMP.

The switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. The hosts may respond with several types of IP multicast messages. Hosts respond to queries with report messages that indicate which groups they want to join or the groups to which they already belong. If a router does not receive a report message within a specified period of time, it will prune that interface from the multicast tree. A host can also submit a join message at any time without waiting for a query from the router. Hosts can also signal when they no longer want to receive traffic for a specific group by sending a leave-group message.

If more than one router on the LAN is performing IP multicasting, one of these is elected as the “querier” and assumes the role of querying for group members. It then propagates the service request up to any neighboring multicast router to ensure that it will continue to receive the multicast service. The parameters described in this section are used to control Layer 3 IGMP and query functions.

**NOTE:** IGMP Protocol Status should be enabled on all the interfaces that need to support downstream multicast hosts (as described in this section).

**NOTE:** IGMP is disabled when multicast routing is disabled (see "Enabling Multicast Routing Globally" on page 568).

### CLI REFERENCES

■"IGMP (Layer 3)" on page 991

### PARAMETERS

These parameters are displayed in the web interface:

■**VLAN** – VLAN interface bound to a primary IP address. (Range: 1-4093)

■**IGMP Protocol Status** – Enables IGMP (including IGMP query functions) on a VLAN interface. (Default: Disabled)

When a multicast routing protocol, such as PIM, is enabled, IGMP is also enabled.

■**IGMP Version** – Configures the IGMP version used on an interface. (Options: Version 1-3; Default: Version 2)

■**Robustness Variable** – Specifies the robustness (or expected packet loss) for this interface. The robustness value is used in calculating the appropriate range for other IGMP variables, such as the Group Membership Interval, as well as the Other Querier Present Interval, and the Startup Query Count (RFC 2236). (Range: 1-255; Default: 2)

Routers adopt the robustness value from the most recently received query. If the querier's robustness variable (QRV) is zero, indicating that the QRV field does not contain a declared robustness value, the switch will set the robustness variable to the value statically configured by this command. If the QRV exceeds 7, the maximum value of the QRV field, the robustness value is set to zero, meaning that this device will not advertise a QRV in any query messages it subsequently sends.

■**Query Interval** – Configures the frequency at which host query messages are sent. (Range: 1-255; Default: 125 seconds)

Multicast routers send host query messages to determine the interfaces that are connected to downstream hosts requesting a specific multicast service. Only the designated multicast router for a subnet sends host query messages, which are addressed to the multicast address 224.0.0.1, and use a time-to-live (TTL) value of 1.

For IGMP Version 1, the designated router is elected according to the multicast routing protocol that runs on the LAN. But for IGMP Version 2 and 3, the designated querier is the lowest IP-addressed multicast router on the subnet.

■**Query Max Response Time** – Configures the maximum response time advertised in IGMP queries. (Range: 0-255 tenths of a second; Default: 10 seconds)

IGMPv1 does not support a configurable maximum response time for query messages. It is fixed at 10 seconds for IGMPv1.

By varying the Query Maximum Response Time, the burstiness of IGMP messages passed on the subnet can be tuned; where larger values make the traffic less bursty, as host responses are spread out over a larger interval.

The number of seconds represented by the maximum response interval must be less than the Query Interval.

■**Last Member Query Interval** – The frequency at which to send IGMP group-specific or IGMPv3 group-source-specific query messages in response to receiving a group-specific or group-source-specific leave message. (Range: 0-255 tenths of a second; Default: 1 second)

When the switch receives an IGMPv2 or IGMPv3 leave message from a host that wants to leave a multicast group, source or channel, it sends a number of group-specific or group-source-specific query messages as defined by the Last Member Query Count at intervals defined by the Last Member Query Interval. If no response is received after this period, the -switch stops forwarding for the group, source or channel.

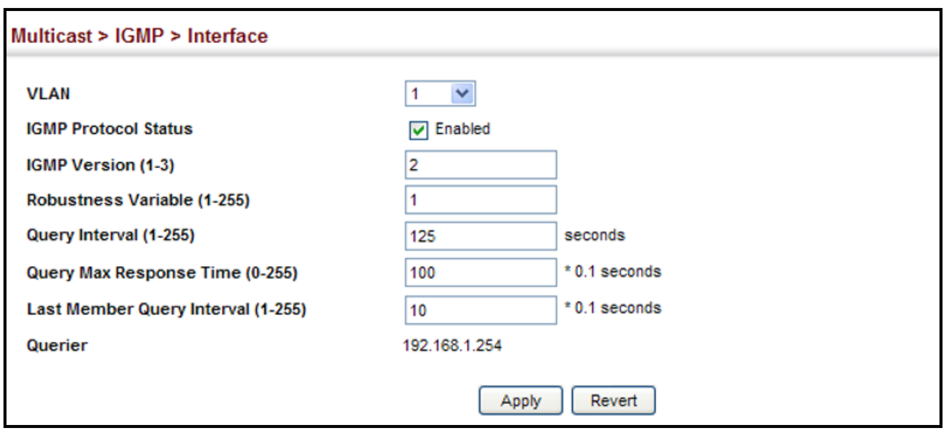
- **Querier** – Device currently serving as the IGMP querier for this multicast service. A querier can only be displayed if IGMP multicasting is enabled, the VLAN for this entry is up, and is configured with a valid IP address.

### WEB INTERFACE

To configure IGMP interface settings:

1. Click Multicast, IGMP, Interface.
2. Select each interface that will support IGMP (Layer 3), and set the required IGMP parameters.
3. Click Apply.

**Figure 22: Configuring IGMP Interface Settings**




## Configuring Static IGMP Group Membership

Use the Multicast > IGMP > Static Group page to manually propagate traffic from specific multicast groups onto the specified VLAN interface.

### CLI REFERENCES

- "ip igmp static-group" on page 995

### COMMAND USAGE

- Group addresses within the entire multicast group address range can be specified. However, if any address within the source-specific multicast (SSM) address range (default 232/8) is specified, but no source address is included, the request to join the multicast group will fail unless the next node up the reverse path tree has statically mapped this group to a specific source address. Also, if an address outside of the SSM address range is specified, and a specific source address is included in the command, the request to join the multicast group will also fail if the next node up the reverse path tree has enabled the PIM-SSM protocol.

- If a static group is configured for an any-source multicast (*,G), a source address cannot subsequently be defined for this group without first deleting the entry.
- If a static group is configured for one or more source-specific multicasts (S,G), an any-source multicast (*,G) cannot subsequently be defined for this group without first deleting all of the associated (S,G) entries.
- The switch supports a maximum of 64 static group entries.

### PARAMETERS

These parameters are displayed in the web interface:

- **VLAN** – VLAN interface to assign as a static member of the specified multicast group. (Range: 1-4093)
- **Static Group Address** – An IP multicast group address. (The group addresses specified cannot be in the range of 224.0.0.1 - 239.255.255.255.)
- **Source Address** – The source address of a multicast server transmitting traffic to the specified multicast group address.

### WEB INTERFACE

To configure static IGMP groups:

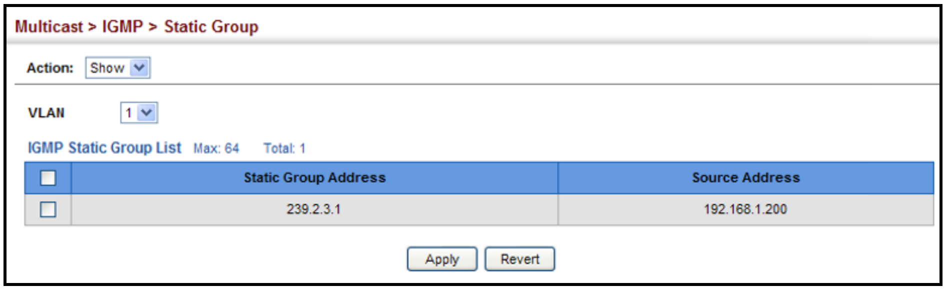
1. Click Multicast, IGMP, Static Group.
2. Select Add from the Action list.
3. Select a VLAN interface to be assigned as a static multicast group member, and then specify the multicast group. If source-specific multicasting is supported by the next hop router in the reverse path tree for the specified multicast group, then the source address should also be specified.
4. Click Apply.

**Figure 23: Configuring Static IGMP Groups**

To display configured static IGMP groups:

1. Click Multicast, IGMP, Static Group.
2. Select Show from the Action list.
3. Click Apply.

**Figure 24: Showing Static IGMP Groups**




## Displaying Multicast Group Information

When IGMP (Layer 3) is enabled on the switch, use the Multicast > IGMP > Group Information pages to display the current multicast groups learned through IGMP. When IGMP (Layer 3) is disabled and IGMP (Layer 2) is enabled, the active multicast groups can be viewed on the Multicast > IGMP Snooping > Forwarding Entry page (see page 392).

### COMMAND USAGE

To display information about multicast groups, IGMP must first be enabled on the interface to which a group has been assigned (see "Configuring IGMP Interface Parameters" on page 401), and multicast routing must be enabled globally on the system (see "Configuring Global Settings for Multicast Routing" on page 568).

### CLI REFERENCES

- "show ip igmp groups" on page 997

### PARAMETERS

These parameters are displayed in the web interface:

*Show Information*

- **VLAN** – VLAN identifier. The selected entry must be a configured IP interface. (Range: 1-4093)

- **Group Address** – IP multicast group address with subscribers directly attached or downstream from the switch.

- **Last Reporter** – The IP address of the source of the last membership report received for this multicast group address on this interface.

- **Up Time** – The time elapsed since this entry was created. (Depending on the elapsed time, information may displayed for w:weeks, d:days, h:hours, m:minutes, or s:seconds.)

- **Expire** – The time remaining before this entry will be aged out. (Default: 260 seconds)

  This parameter displays “stopped” if the Group Mode is INCLUDE.

- **V1 Timer** – The time remaining until the switch assumes that there are no longer any IGMP Version 1 members on the IP subnet attached to this interface.

  - If the switch receives an IGMP Version 1 Membership Report, it sets a timer to note that there are Version 1 hosts present which are members of the group for which it heard the report.

  - If there are Version 1 hosts present for a particular group, the switch will ignore any Leave Group messages that it receives for that group.

*Show Detail*

The following additional information is displayed on this page:

- **VLAN** – VLAN identifier. The selected entry must be a configured IP interface. (Range: 1-4093)

- **Group Address** – IP multicast group address with subscribers directly attached or downstream from the switch, or a static multicast group assigned to this interface.

- **Interface** – The interface on the switch that has received traffic directed to the multicast group address.

- **Up Time** – The time elapsed since this entry was created. (Depending on the elapsed time, information may displayed for w:weeks, d:days, h:hours, m:minutes, or s:seconds.)

- **Group Mode** – In INCLUDE mode, reception of packets sent to the specified multicast address is requested only from those IP source addresses listed in the source-list parameter. In EXCLUDE mode, reception of packets sent to the given multicast address is requested from all IP source addresses, except for those listed in the source-list parameter and for any other sources where the source timer status has expired.

- **Group Source List** – A list of zero or more IP unicast addresses from which multicast reception is desired or not desired, depending on the filter mode.

  - **Source Address** – The address of one of the multicast servers transmitting traffic to the specified group.

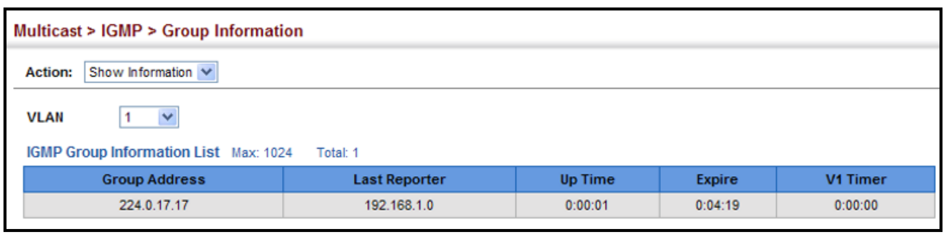
- **Up Time** – The time elapsed since this entry was created. (Depending on the elapsed time, information may displayed for w:weeks, d:days, h:hours, m:minutes, or s:seconds.)
- **V3 Expire** – The time remaining before this entry will be aged out. The V3 label indicates that the expire time is only provided for sources learned through IGMP Version 3. (The default is 260 seconds.)
- **Forward** – Indicates whether or not traffic will be forwarded from the multicast source.

### WEB INTERFACE

To display the current multicast groups learned through IGMP:

1. Click Multicast, IGMP, Group Information.
2. Select Show Information from the Action list.
3. Select a VLAN. The selected entry must be a configured IP interface.

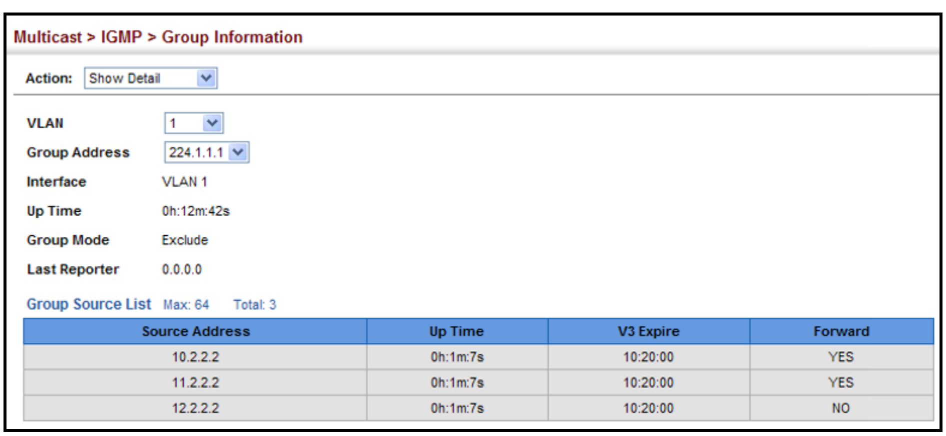
**Figure 25: Displaying Multicast Groups Learned from IGMP** (Information)




To display detailed information about the current multicast groups learned through IGMP:

1. Click Multicast, IGMP, Group Information.
2. Select Show Detail from the Action list.
3. Select a VLAN. The selected entry must be a configured IP interface.

**Figure 26: Displaying Multicast Groups Learned from IGMP** (Detail)

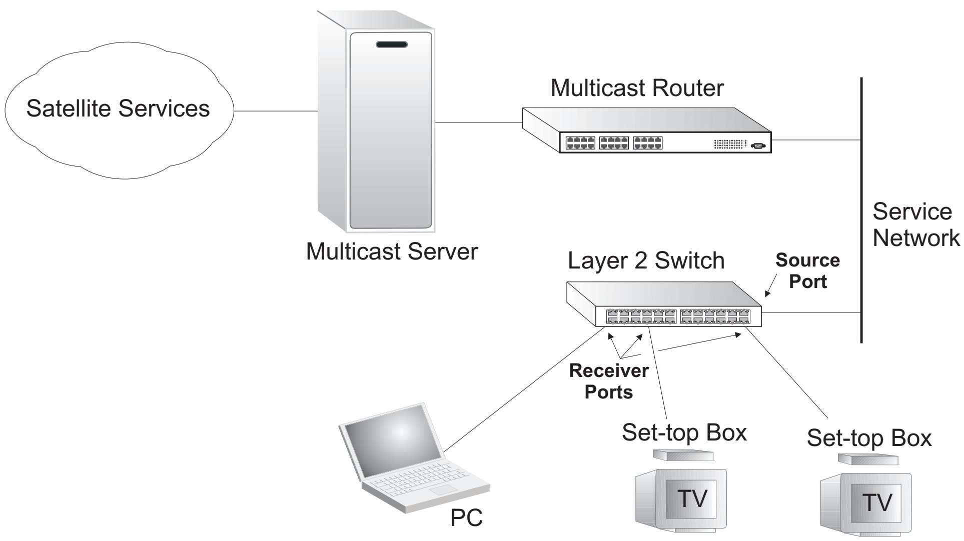


# MULTICAST VLAN REGISTRATION

Multicast VLAN Registration (MVR) is a protocol that controls access to a single network-wide VLAN most commonly used for transmitting multicast traffic (such as television channels or video-on-demand) across a service provider’s network. Any multicast traffic entering an MVR VLAN is sent to all attached subscribers. This protocol can significantly reduce to processing overhead required to dynamically monitor and establish the distribution tree for a normal multicast VLAN. This makes it possible to support common multicast services over a wide part of the network without having to use any multicast routing protocol.

MVR maintains the user isolation and data security provided by VLAN segregation by passing only multicast traffic into other VLANs to which the subscribers belong. Even though common multicast streams are passed onto different VLAN groups from the MVR VLAN, users in different IEEE 802.1Q or private VLANs cannot exchange any information (except through upper-level routing services).

**Figure 27: MVR Concept**




### COMMAND USAGE

■General Configuration Guidelines for MVR:

1. Enable MVR globally on the switch, select the MVR VLAN, and add the multicast groups that will stream traffic to attached hosts (see "Configuring Global MVR Settings" on page 409).
2. Set the interfaces that will join the MVR as source ports or receiver ports (see "Configuring MVR Interface Status" on page 411).
3. For multicast streams that will run for a long term and be associated with a stable set of hosts, you can statically bind the multicast group to the participating interfaces (see "Assigning Static Multicast Groups to Interfaces" on page 413).

■Although MVR operates on the underlying mechanism of IGMP snooping, the two features operate independently of each other. One can be enabled or disabled without affecting the behavior of the other. However, if IGMP snooping and MVR are both enabled, MVR reacts only to join and leave messages from multicast groups configured under MVR. Join and leave messages from all other multicast groups are managed by IGMP snooping. Also, note that only IGMP version 2 or 3 hosts can issue multicast join or leave messages.

## Configuring Global MVR Settings

Use the Multicast > MVR (Configure General) page to enable MVR globally on the switch, and select the VLAN that will serve as the sole channel for common multicast streams supported by the service provider.

#### CLI REFERENCES

- "Multicast VLAN Registration" on page 984

#### PARAMETERS

These parameters are displayed in the web interface:

- **MVR Status** – When MVR is enabled on the switch, any multicast data associated with an MVR group is sent from all designated source ports, to all receiver ports that have registered to receive data from that multicast group. (Default: Disabled)
- **MVR VLAN** – Identifier of the VLAN that serves as the channel for streaming multicast services using MVR. MVR source ports should be configured as members of the MVR VLAN (see "Adding Static Members to VLANs" on page 142), but MVR receiver ports should not be manually configured as members of this VLAN. (Default: 1)
- **MVR Running Status** – Indicates whether or not all necessary conditions in the MVR environment are satisfied. Running status is Active as long as MVR is enabled, the specified MVR VLAN exists, and a source port with a valid link has been configured (see "Configuring MVR Interface Status" on page 411).
- **MVR Current Groups** – The number of multicast groups currently assigned to the MVR VLAN.
- **MVR Max Supported Groups** – The maximum number of multicast groups supported by this switch.

  IGMP snooping and MVR share a maximum number of 255 groups. Any multicast streams received in excess of this limitation will be flooded to all ports in the associated VLAN.
- **Upstream Source IP** – The source IP address assigned to all MVR control packets sent upstream. (Default: Null source IP address)

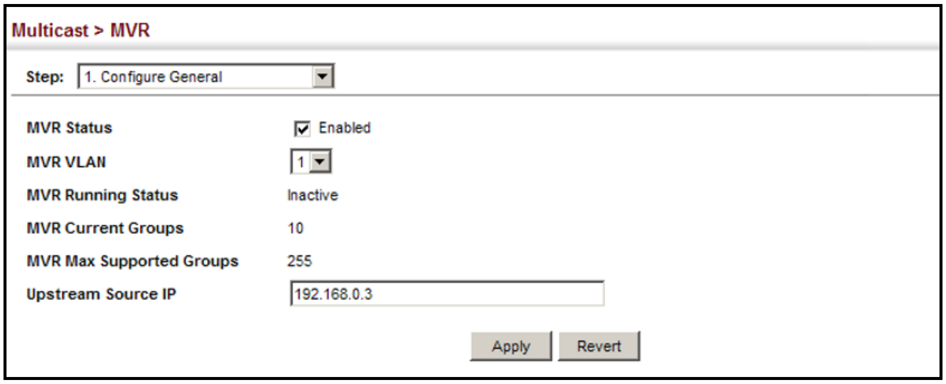
#### WEB INTERFACE

To configure global settings for MVR:

1. Click Multicast, MVR.
2. Select Configure General from the Action list.
3. Enable MVR globally on the switch, and select the MVR VLAN.

**4.** Click Apply.

**Figure 28: Configuring Global Settings for MVR**




## Configuring the MVR Group Range

Use the Multicast > MVR (Configure Group Range) page to assign the multicast group address for each service to the MVR VLAN.

### CLI REFERENCES

■ "Multicast VLAN Registration" on page 984

### COMMAND USAGE

IGMP snooping and MVR share a maximum number of 255 groups. Any multicast streams received in excess of this limitation will be flooded to all ports in the associated VLAN.

### PARAMETERS

These parameters are displayed in the web interface:

■ **MVR Group IP** – IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255; Default: no groups are assigned to the MVR VLAN)

Any multicast data sent to this address is sent to all source ports on the switch and all receiver ports that have elected to receive data on that multicast address.

The IP address range of 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.

IGMP snooping and MVR share a maximum number of 255 groups. Any multicast streams received in excess of this limitation will be flooded to all ports in the associated VLAN.

■ **Count** – The number of contiguous MVR group addresses. (Range: 1-255; Default: 0)

### WEB INTERFACE

To configure multicast groups for the MVR VLAN:

**1.** Click Multicast, MVR.

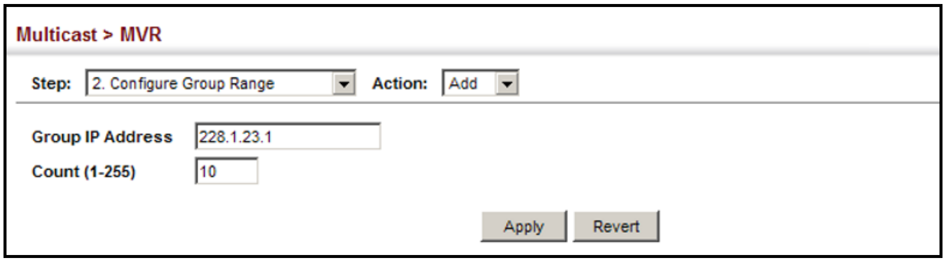
**2.** Select Configure Group Range from the Step list.

3. Select Add from the Action list.

4. Add the multicast groups that will stream traffic to participating hosts.

5. Click Apply.

**Figure 29: Configuring the Group Range for MVR**



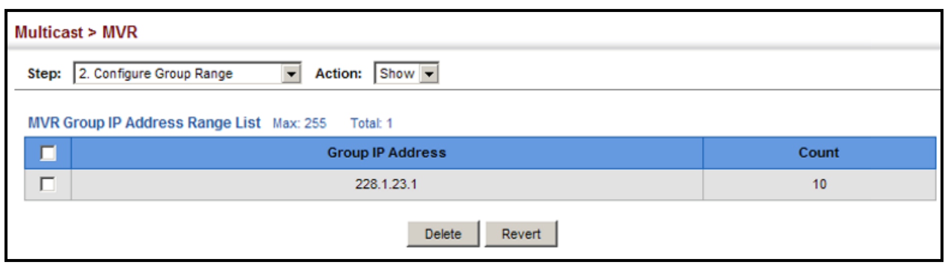

To show the multicast groups assigned to the MVR VLAN:

1. Click Multicast, MVR.

2. Select Configure Group Range from the Step list.

3. Select Show from the Action list.

**Figure 30: Showing the Configured Group Range for MVR**




## Configuring MVR Interface Status

Use the Multicast > MVR (Configure Interface) page to configure each interface that participates in the MVR protocol as a source port or receiver port. If you are sure that only one subscriber attached to an interface is receiving multicast services, you can enable the immediate leave function.

### CLI References

■ "Multicast VLAN Registration" on page 984

### Command Usage

■ A port configured as an MVR receiver or source port can join or leave multicast groups configured under MVR. However, note that these ports can also use IGMP snooping to join or leave any other multicast groups using the standard rules for multicast filtering.

■ Receiver ports can belong to different VLANs, but should not be configured as a member of the MVR VLAN. IGMP snooping is used to allow a receiver port to dynamically join or leave multicast groups within an MVR VLAN. Multicast groups can also be statically assigned to a receiver port (see "Assigning Static Multicast Groups to Interfaces" on page 413).

Receiver ports should not be statically configured as a member of the MVR VLAN. If so configured, its MVR status will be inactive.

- One or more interfaces may be configured as MVR source ports. A source port is able to both receive and send data for configured MVR groups or for groups which have been statically assigned (see "Assigning Static Multicast Groups to Interfaces" on page 413).

  All source ports must belong to the MVR VLAN.

  Subscribers should not be directly connected to source ports.

- Immediate leave applies only to receiver ports. When enabled, the receiver port is immediately removed from the multicast group identified in the leave message. When immediate leave is disabled, the switch follows the standard rules by sending a query message to the receiver port and waiting for a response to determine if there are any remaining subscribers for that multicast group before removing the port from the group list.
  - Using immediate leave can speed up leave latency, but should only be enabled on a port attached to one multicast subscriber to avoid disrupting services to other group members attached to the same interface.
  - Immediate leave does not apply to multicast groups which have been statically assigned to a port.

**PARAMETERS**

These parameters are displayed in the web interface:

- **Port** – Port identifier.
- **Type** – The following interface types are supported:
  - **Source** – An uplink port that can send and receive multicast data for the groups assigned to the MVR VLAN. Note that the source port must be manually configured as a member of the MVR VLAN (see "Adding Static Members to VLANs" on page 142).
  - **Receiver** – A subscriber port that can receive multicast data sent through the MVR VLAN. Any port configured as an receiver port will be dynamically added to the MVR VLAN when it forwards an IGMP report or join message from an attached host requesting any of the designated multicast services supported by the MVR VLAN. Just remember that only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned (see "Assigning Static Multicast Groups to Interfaces" on page 413).
  - **Non-MVR** – An interface that does not participate in the MVR VLAN. (This is the default type.)
- **Oper. Status** – Shows the link status.
- **MVR Status** – Shows the MVR status. MVR status for source ports is “Active” if MVR is globally enabled on the switch. MVR status for receiver ports is “Active”

only if there are subscribers receiving multicast traffic from one of the MVR groups, or a multicast group has been statically assigned to an interface.

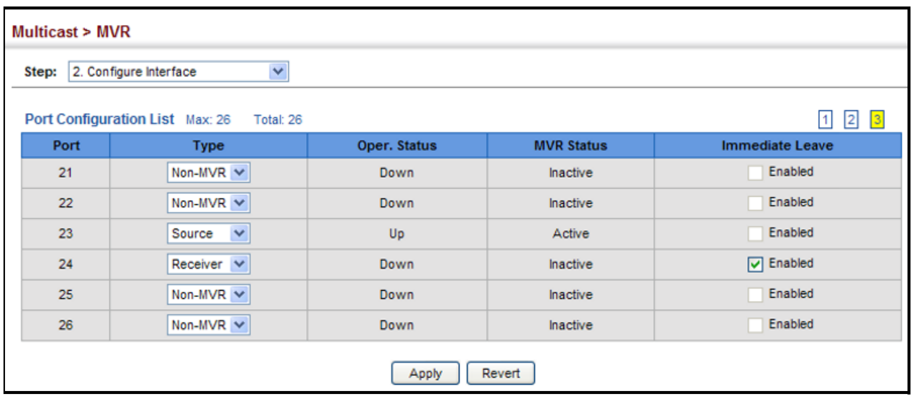
- **Immediate Leave** – Configures the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group. (This option only applies to an interface configured as an MVR receiver.)

### WEB INTERFACE

To configure interface settings for MVR:

1. Click Multicast, MVR.
2. Select Configure Interface from the Action list.
3. Set each port that will participate in the MVR protocol as a source port or receiver port, and optionally enable Immediate Leave on any receiver port to which only one subscriber is attached.
4. Click Apply.

**Figure 31: Configuring Interface Settings for MVR**




## Assigning Static Multicast Groups to Interfaces

Use the Multicast > MVR (Configure Static Group Member) page to statically bind multicast groups to a port which will receive long-term multicast streams associated with a stable set of hosts.

### CLI REFERENCES

- "mvr vlan group" on page 988

### PARAMETERS

These parameters are displayed in the web interface:

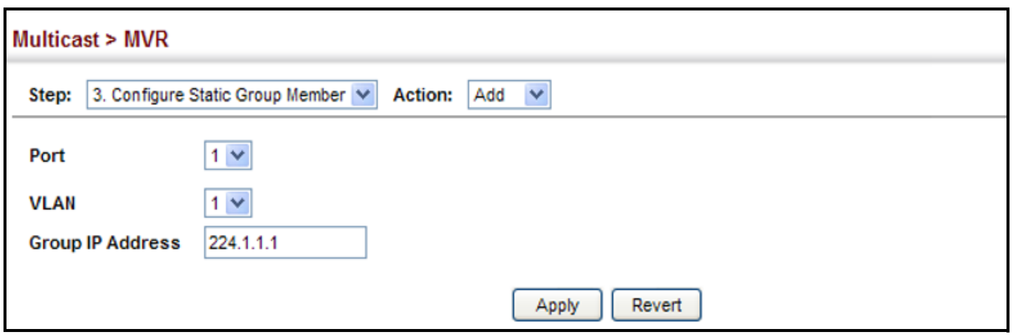
- **Port** – Port identifier.
- **VLAN** – VLAN identifier
- **Group IP Address** – Defines a multicast service sent to the selected port. Multicast groups must be assigned from the MVR group range configured on the Configure General page.

### WEB INTERFACE

To assign a static MVR group to a port:

1. Click Multicast, MVR.
2. Select Configure Static Group Member from the Step list.
3. Select Add from the Action list.
4. Select a VLAN and port member to receive the multicast stream, and then enter the multicast group address.
5. Click Apply.

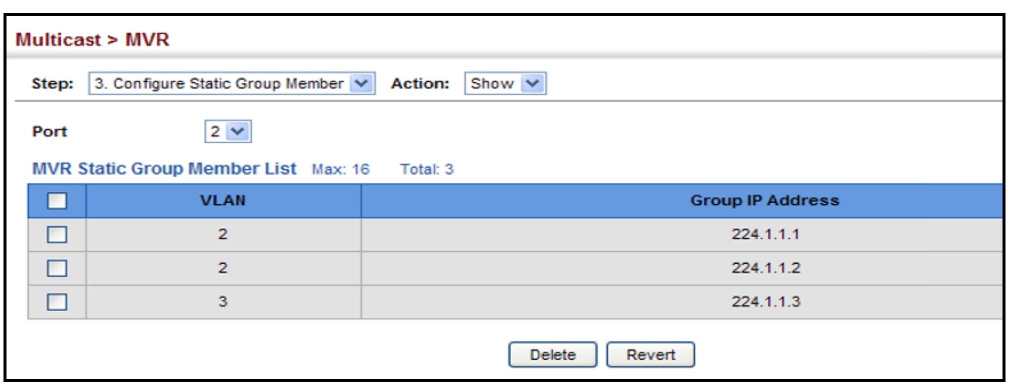
**Figure 32: Assigning Static MVR Groups to a Port**




To show the static MVR groups assigned to a port:

1. Click Multicast, MVR.
2. Select Configure Static Group Member from the Step list.
3. Select Show from the Action list.
4. Select the port for which to display this information.

**Figure 33: Showing the Static MVR Groups Assigned to a Port**



### Showing Multicast Groups Assigned to Interfaces

Use the Multicast > MVR (Show Member) page to show the multicast groups either statically or dynamically assigned to the MVR VLAN on each interface.

**CLI REFERENCES**

■"show mvr" on page 989

**PARAMETERS**

These parameters are displayed in the web interface:

**Group IP Address** – Multicast groups assigned to the MVR VLAN.

**Source IP Address** – Indicates the source address of the multicast service, or displays an asterisk if the group address has been statically assigned.

**VLAN** – Indicates the MVR VLAN receiving the multicast service.

**Forwarding Port** – Shows the interfaces with subscribers for multicast services provided through the MVR VLAN. Also shows the VLAN through which the service is received. Note that this may be different from the MVR VLAN if the group address has been statically assigned.

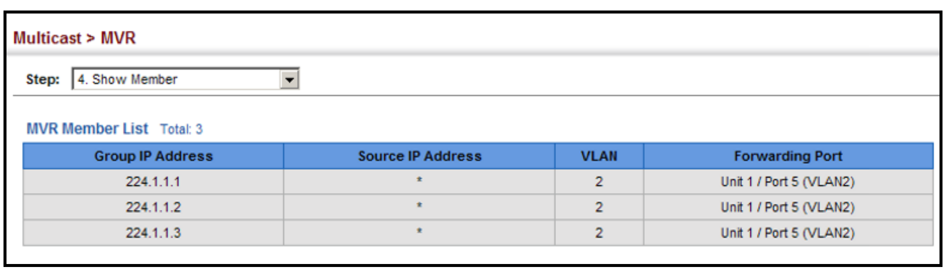
**WEB INTERFACE**

To show all MVR groups assigned to a port:

**1.** Click Multicast, MVR.

**2.** Select Show Member from the Step list.

**Figure 34: Showing All MVR Groups Assigned to a Port**



# 17 IP CONFIGURATION

This chapter describes how to configure an initial IP interface for management access to the switch over the network. This switch supports both IP Version 4 and Version 6, and can be managed simultaneously through either of these address types. You can manually configure a specific IPv4 or IPv6 address or direct the switch to obtain an IPv4 address from a BOOTP or DHCP server when it is powered on. An IPv6 global unicast or link-local address can be manually configured, or a link-local address can be dynamically generated.

This chapter provides information on network functions including:

- IPv4 Configuration – Sets an IPv4 address for management access.
- IPv6 Configuration – Sets an IPv6 address for management access.

## SETTING THE SWITCH'S IP ADDRESS (IP VERSION 4)

Use the IP > General > Routing Interface (Add) page to configure an IPv4 address for the switch. An IPv4 address is obtained via DHCP by default for VLAN 1. To configure a static address, you need to change the switch's default settings to values that are compatible with your network. You may also need to a establish a default gateway between the switch and management stations that exist on another network segment (if no routing protocols are enabled).

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

### CLI REFERENCES

- "Basic IPv4 Configuration" on page 1068
- "DHCP Client" on page 1039

### COMMAND USAGE

- This section describes how to configure a single local interface for initial access to the switch. To configure multiple IP interfaces, set up an IP interface for each VLAN.
- Once an IP address has been assigned to an interface, routing between different interfaces on the switch is enabled.
- To enable routing between interfaces defined on this switch and external network interfaces, you must configure static routes (page 449) or use dynamic routing; i.e., RIP, OSPFv2 or OSPFv3 (page 486, 504 or 1175 respectively).

- The precedence for configuring IP interfaces is the IP > General > Routing Interface (Add) menu, static routes (page 449), and then dynamic routing.

### PARAMETERS

These parameters are displayed in the web interface:

- **VLAN** – ID of the configured VLAN (1-4093). By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address.

- **IP Address Mode** – Specifies whether IP functionality is enabled via manual configuration (Static), Dynamic Host Configuration Protocol (DHCP), or Boot Protocol (BOOTP). If DHCP/BOOTP is enabled, IP will not function until a reply has been received from the server. Requests will be broadcast periodically by the switch for an IP address. DHCP/BOOTP responses can include the IP address, subnet mask, and default gateway. (Default: DHCP)

- **IP Address Type** – Specifies a primary or secondary IP address. An interface can have only one primary IP address, but can have many secondary IP addresses. In other words, secondary addresses need to be specified if more than one IP subnet can be accessed through this interface. For initial configuration, set this parameter to Primary. (Options: Primary, Secondary; Default: Primary)

  Note that a secondary address cannot be configured prior to setting the primary IP address, and the primary address cannot be removed if a secondary address is still present. Also, if any router in a network segment uses a secondary address, all other routers in that segment must also use a secondary address from the same network or subnet address space.

- **IP Address** – IP Address of the VLAN. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: 0.0.0.0)

**NOTE:** You can manage the switch through any configured IP interface.

- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets.

- **Restart DHCP** – Requests a new IP address from the DHCP server for all enabled VLANs.

### WEB INTERFACE

To set a static address for the switch:

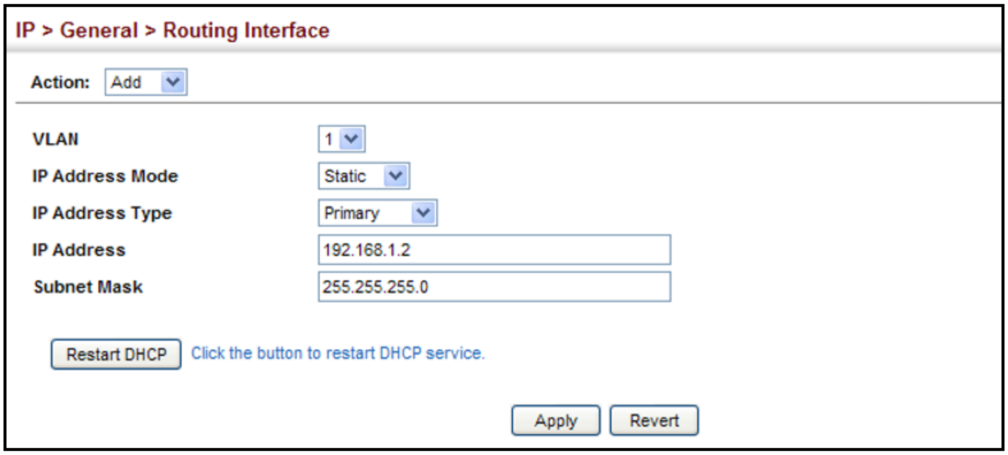
1. Click IP, General, Routing Interface.

2. Select Add from the Action list.

3. Select any configured VLAN, set IP Address Mode to "Static," set IP Address Type to "Primary" if no address has yet been configured for this interface, and then enter the IP address and subnet mask.

4. Click Apply.

**Figure 1: Configuring a Static IPv4 Address**

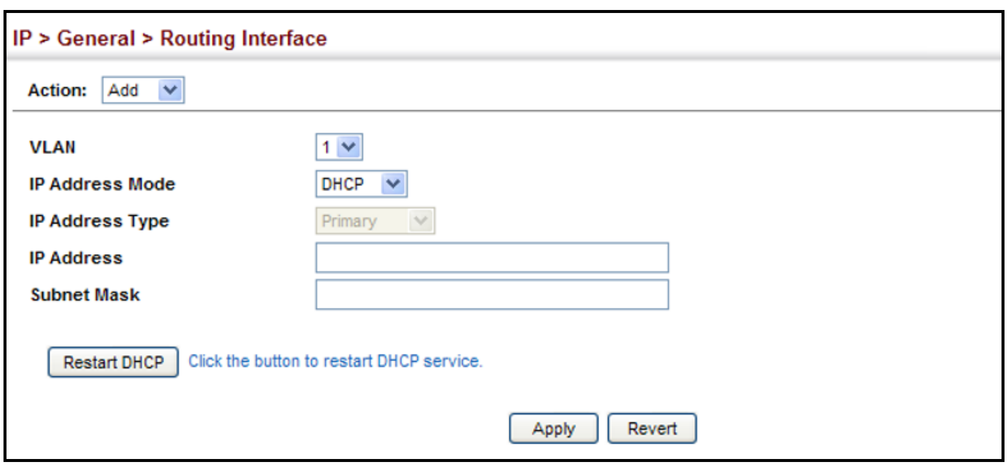



To obtain an dynamic address through DHCP/BOOTP for the switch:

1. Click IP, General, Routing Interface.
2. Select Add from the Action list.
3. Select any configured VLAN, and set IP Address Mode to "BOOTP" or "DHCP."
4. Click Apply to save your changes.

IP will be enabled but will not function until a BOOTP or DHCP reply is received. Requests are broadcast every few minutes using exponential backoff until IP configuration information is obtained from a BOOTP or DHCP server.

**Figure 2: Configuring a Dynamic IPv4 Address**




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

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

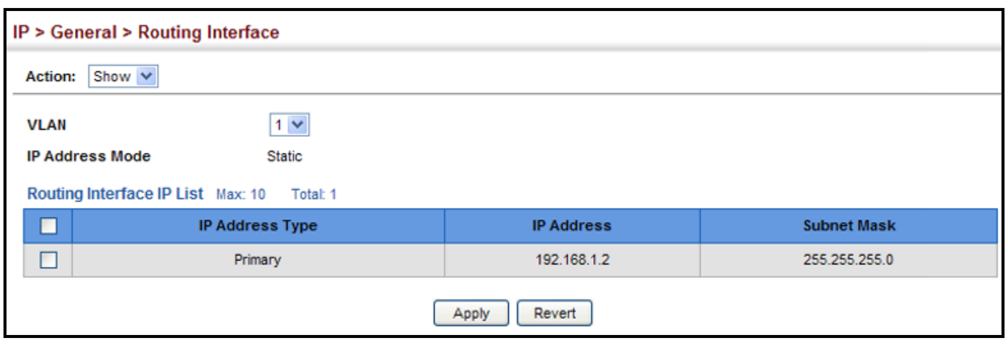
**Renewing DCHP** – DHCP may lease addresses to clients indefinitely or for a specific period of time. If the address expires or the switch is moved to another network segment, you will lose management access to the switch. In this case, you can reboot the switch or submit a client request to restart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

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

To show the address configured for an interface:

1. Click IP, General, Routing Interface.
2. Select Add from the Action list.
3. Select an entry from the VLAN list.

**Figure 3: Showing the Configured IP Address for an Interface**




## SETTING THE SWITCH'S IP ADDRESS (IP VERSION 6)

This section describes how to configure an initial IPv6 interface for management access over the network, or for creating an interface to multiple subnets. This switch supports both IPv4 and IPv6, and can be managed through either of these address types. For information on configuring the switch with an IPv4 address, see "Setting the Switch's IP Address (IP Version 4)" on page 417.

### COMMAND USAGE

- IPv6 includes two distinct address types – link-local unicast and global unicast. A link-local address makes the switch accessible over IPv6 for all devices attached to the same local subnet. Management traffic using this kind of address cannot be passed by any router outside of the subnet. A link-local address is easy to set up, and may be useful for simple networks or basic troubleshooting tasks. However, to connect to a larger network with multiple segments, the switch must be configured with a global unicast address.

- An IPv6 global unicast or link-local address can be manually configured (using the Add IPv6 Address page), or a link-local address can be dynamically generated (using the Configure Interface page).

## Configuring the IPv6 Default Gateway

Use the IP > IPv6 Configuration (Configure Global) page to configure an IPv6 default gateway for the switch.

### CLI References

■"ipv6 default-gateway" on page 1082

### Parameters

These parameters are displayed in the web interface:

■**Default Gateway** – Sets the IPv6 address of the default next hop router to use when no routing information is known about an IPv6 address.

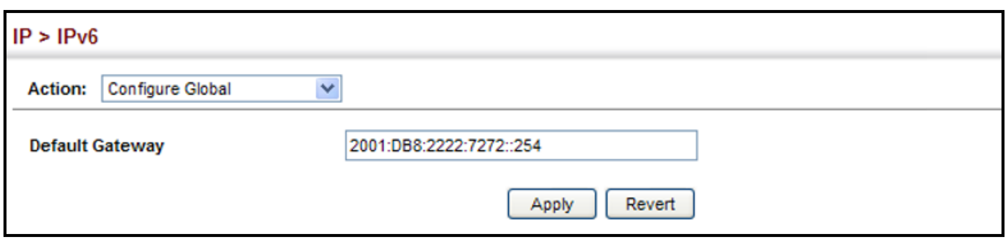
- If no routing protocol is enabled or static route defined, you must define a gateway if the target device is located in a different subnet.
- If a routing protocol is enabled (page 485), you can still define a static route (page 449) to ensure that traffic to the designated address or subnet passes through a preferred gateway.
- An IPv6 default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the switch.

### Web Interface

To configure an IPv6 default gateway for the switch:

1. Click IP, IPv6 Configuration.
2. Select Configure Global from the Action list.
3. Enter the IPv6 default gateway.
4. Click Apply.

**Figure 4: Configuring the IPv6 Default Gateway**




## Configuring IPv6 Interface Settings

Use the IP > IPv6 Configuration (Configure Interface) page to configure general IPv6 settings for the selected VLAN, including explicit configuration of a link local interface address, the MTU size, and neighbor discovery protocol settings for duplicate address detection and the neighbor solicitation interval.

### CLI References

■"IPv6 Interface" on page 1081

■"DHCP Client" on page 1039

### Command Usage

- The switch must be configured with a link-local address. The option to explicitly enable IPv6 creates a link-local address, but will not generate a global IPv6 address. The global unicast address must be manually configured (see "Configuring an IPv6 Address" on page 424).

- IPv6 Neighbor Discovery Protocol supersedes IPv4 Address Resolution Protocol in IPv6 networks. IPv6 nodes on the same network segment use Neighbor Discovery to discover each other's presence, to determine each other's link-layer addresses, to find routers and to maintain reachability information about the paths to active neighbors. The key parameters used to facilitate this process are the number of attempts made to verify whether or not a duplicate address exists on the same network segment, and the interval between neighbor solicitations used to verify reachability information.

### Parameters

These parameters are displayed in the web interface:

- **VLAN** – ID of a configured VLAN which is to be used for management access, or as a standard interface for a subnet. By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address. (Range: 1-4093)

- **Address Autoconfig** – This configuration option is not supported for Layer 3 routers.

- **Enable IPv6 Explicitly** – Enables IPv6 on an interface. Note that when an explicit address is assigned to an interface, IPv6 is automatically enabled, and cannot be disabled until all assigned addresses have been removed. (Default: Disabled)

  Disabling this parameter does not disable IPv6 for an interface that has been explicitly configured with an IPv6 address.

- **MTU** – Sets the size of the maximum transmission unit (MTU) for IPv6 packets sent on an interface. (Range: 1280-65535 bytes; Default: 1500 bytes)

  - The maximum value set by this command cannot exceed the MTU of the physical interface, which is currently fixed at 1500 bytes.
  - If a non-default value is configured, an MTU option is included in the router advertisements sent from this device. This option is provided to ensure that all nodes on a link use the same MTU value in cases where the link MTU is not otherwise well known.
  - IPv6 routers do not fragment IPv6 packets forwarded from other routers. However, traffic originating from an end-station connected to an IPv6 router may be fragmented.
  - All devices on the same physical medium must use the same MTU in order to operate correctly.
  - IPv6 must be enabled on an interface before the MTU can be set. If an IPv6 address has not been assigned to the switch, “N/A” is displayed in the MTU field.

- **ND DAD Attempts** – The number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection. (Range: 0-600, Default: 2)
  - Configuring a value of 0 disables duplicate address detection.
  - Duplicate address detection determines if a new unicast IPv6 address already exists on the network before it is assigned to an interface.
  - Duplicate address detection is stopped on any interface that has been suspended (see "Configuring VLAN Groups" on page 140). While an interface is suspended, all unicast IPv6 addresses assigned to that interface are placed in a "pending" state. Duplicate address detection is automatically restarted when the interface is administratively re-activated.
  - An interface that is re-activated restarts duplicate address detection for all unicast IPv6 addresses on the interface. While duplicate address detection is performed on the interface's link-local address, the other IPv6 addresses remain in a "tentative" state. If no duplicate link-local address is found, duplicate address detection is started for the remaining IPv6 addresses.
  - If a duplicate address is detected, it is set to "duplicate" state, and a warning message is sent to the console. If a duplicate link-local address is detected, IPv6 processes are disabled on the interface. If a duplicate global unicast address is detected, it is not used. All configuration commands associated with a duplicate address remain configured while the address is in "duplicate" state.
  - If the link-local address for an interface is changed, duplicate address detection is performed on the new link-local address, but not for any of the IPv6 global unicast addresses already associated with the interface.

- **ND NS Interval** – The interval between transmitting IPv6 neighbor solicitation messages on an interface. (Range: 1000-3600000 milliseconds;

  Default: 1000 milliseconds is used for neighbor discovery operations,
  0 milliseconds is advertised in router advertisements.

  This attribute specifies the interval between transmitting neighbor solicitation messages when resolving an address, or when probing the reachability of a neighbor. Therefore, avoid using very short intervals for normal IPv6 operations.

  When a non-default value is configured, the specified interval is used both for router advertisements and by the router itself.

**Restart DHCPv6** – DHCPv6 stateful configuration of IP address prefixes is not supported in the current software release. If the router advertisements have the "other stateful configuration" flag set, the switch will attempt to acquire other non-address configuration information (such as a default gateway) from a DHCPv6 server.

### WEB INTERFACE

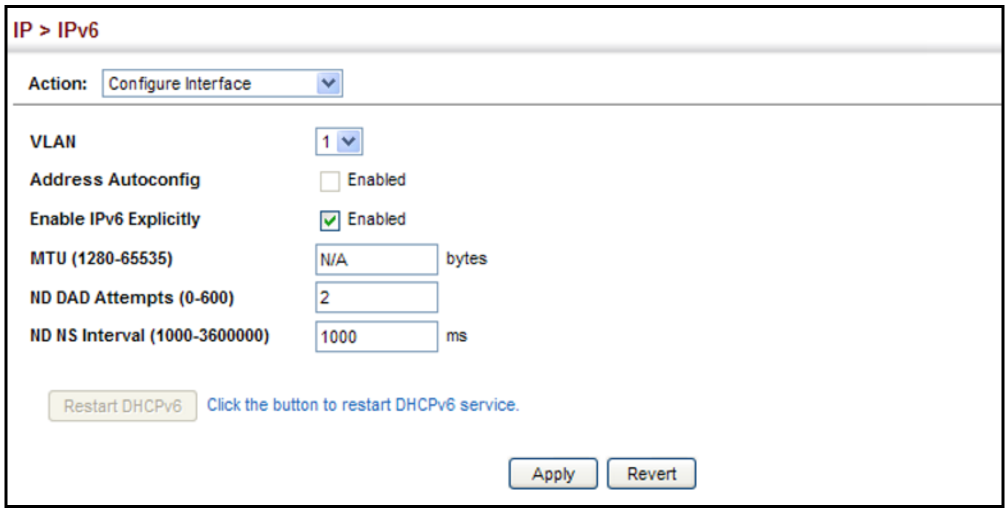
To general IPv6 settings for the switch:

1. Click IP, IPv6 Configuration.
2. Select Configure Interface from the Action list.
3. Specify the VLAN to configure,

**4.** Select Enable IPv6 Explicitly to automatically configure a link-local address and enable IPv6 on the selected interface. (To manually configure the link-local address, use the Add IPv6 Address page.) Set the MTU size, the maximum number of duplicate address detection messages, and the neighbor solicitation message interval.

**5.** Click Apply.

**Figure 5: Configuring General Settings for an IPv6 Interface**




## Configuring an IPv6 Address

Use the IP > IPv6 Configuration (Add IPv6 Address) page to configure an initial IPv6 interface for management access over the network, or for creating an interface to multiple subnets.

### CLI References

■ "IPv6 Interface" on page 1081

### Command Usage

■ All IPv6 addresses must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

■ The switch must always be configured with a link-local address. Therefore, explicitly enabling IPv6 (see "Configuring IPv6 Interface Settings" on page 421) or manually assigning a global unicast address will also automatically generate a link-local unicast address. The prefix length for a link-local address is fixed at 64 bits, and the host portion of the default address is based on the modified EUI-64 (Extended Universal Identifier) form of the interface identifier (i.e., the physical MAC address). Alternatively, you can manually configure the link-local address by entering the full address with the network prefix FE80.

■ To connect to a larger network with multiple subnets, you must configure a global unicast address. There are several alternatives to configuring this address type:

- ◆ It can be manually configured by specifying the entire network prefix and prefix length, and using the EUI-64 form of the interface identifier to automatically create the low-order 64 bits in the host portion of the address.
- ◆ You can also manually configure the global unicast address by entering the full address and prefix length.

■ You can configure multiple IPv6 global unicast addresses per interface, but only one link-local address per interface.

■ If a duplicate link-local address is detected on the local segment, this interface is disabled and a warning message displayed on the console. If a duplicate global unicast address is detected on the network, the address is disabled on this interface and a warning message displayed on the console.

■ When an explicit address is assigned to an interface, IPv6 is automatically enabled, and cannot be disabled until all assigned addresses have been removed.

**PARAMETERS**

These parameters are displayed in the web interface:

■ **VLAN** – ID of a configured VLAN which is to be used for management access, or for creating an interface to multiple subnets. By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address. (Range: 1-4093)

■ **Address Type** – Defines the address type configured for this interface.

- ◆ **Global** – Configures an IPv6 global unicast address with a full IPv6 address including the network prefix and host address bits, followed by a forward slash, and a decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).
- ◆ **EUI-64** (Extended Universal Identifier) – Configures an IPv6 address for an interface using an EUI-64 interface ID in the low order 64 bits.

  ◆ When using EUI-64 format for the low-order 64 bits in the host portion of the address, the value entered in the IPv6 Address field includes the network portion of the address, and the prefix length indicates how many contiguous bits (starting at the left) of the address comprise the prefix (i.e., the network portion of the address). Note that the value specified in the IPv6 Address field may include some of the high-order host bits if the specified prefix length is less than 64 bits. If the specified prefix length exceeds 64 bits, then the bits used in the network portion of the address will take precedence over the interface identifier.

  ◆ IPv6 addresses are 16 bytes long, of which the bottom 8 bytes typically form a unique host identifier based on the device's MAC address. The EUI-64 specification is designed for devices that use an extended 8-byte MAC address. For devices that still use a 6-byte MAC address (also known as EUI-48 format), it must be converted into EUI-64 format by inverting the universal/local bit in the address and inserting the hexadecimal number FFFE between the upper and lower three bytes of the MAC address.

For example, if a device had an EUI-48 address of 28-9F-18-1C-82-35, the global/local bit must first be inverted to meet EUI-64 requirements (i.e., 1 for globally defined addresses and 0 for locally defined addresses), changing 28 to 2A. Then the two bytes FFFE are inserted between the OUI (i.e., organizationally unique identifier, or company identifier) and the rest of the address, resulting in a modified EUI-64 interface identifier of 2A-9F-18-FF-FE-1C-82-35.

◆This host addressing method allows the same interface identifier to be used on multiple IP interfaces of a single device, as long as those interfaces are attached to different subnets.

◆ **Link Local** – Configures an IPv6 link-local address.

◆The address prefix must be FE80.

◆You can configure only one link-local address per interface.

◆The specified address replaces a link-local address that was automatically generated for the interface.

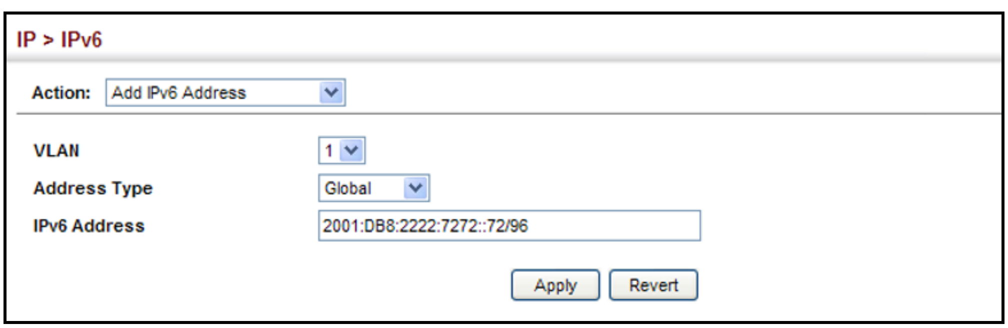
■**IPv6 Address** – IPv6 address assigned to this interface.

**WEB INTERFACE**

To configure an IPv6 address:

1. Click IP, IPv6 Configuration.
2. Select Add IPv6 Address from the Action list.
3. Specify the VLAN to configure, select the address type, and then enter an IPv6 address and prefix length.
4. Click Apply.

**Figure 6: Configuring an IPv6 Address**




## Showing IPv6 Addresses

Use the IP > IPv6 Configuration (Show IPv6 Address) page to display the IPv6 addresses assigned to an interface.

**CLI REFERENCES**

■"show ipv6 interface" on page 1089

### PARAMETERS

These parameters are displayed in the web interface:

- **VLAN** – ID of a configured VLAN which is to be used for management access, or for creating an interface to multiple subnets. By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address. (Range: 1-4093)

- **IP Address Type** – The address type (Global, EUI-64, Link Local).

- **IP Address** – An IPv6 address assigned to this interface.

  In addition to the unicast addresses assigned to an interface, a node is also required to listen to the all-nodes multicast addresses FF01::1 (interface-local scope) and FF02::1 (link-local scope).

  FF01::1/16 is the transient interface-local multicast address for all attached IPv6 nodes, and FF02::1/16 is the link-local multicast address for all attached IPv6 nodes. The interface-local multicast address is only used for loopback transmission of multicast traffic. Link-local multicast addresses cover the same types as used by link-local unicast addresses, including all nodes (FF02::1), all routers (FF02::2), and solicited nodes (FF02::1:FFXX:XXXX) as described below.

  A node is also required to compute and join the associated solicited-node multicast addresses for every unicast and anycast address it is assigned. IPv6 addresses that differ only in the high-order bits, e.g. due to multiple high-order prefixes associated with different aggregations, will map to the same solicited-node address, thereby reducing the number of multicast addresses a node must join. In this example, FF02::1:FF90:0/104 is the solicited-node multicast address which is formed by taking the low-order 24 bits of the address and appending those bits to the prefix.

  Note that the solicited-node multicast address (link-local scope FF02) is used to resolve the MAC addresses for neighbor nodes since IPv6 does not support the broadcast method used by the Address Resolution Protocol in IPv4.

  These additional addresses are displayed by the CLI (see "show ip interface" on page 1071).

- **Configuration Mode** – Indicates if this address was automatically generated for manually configured.

### WEB INTERFACE

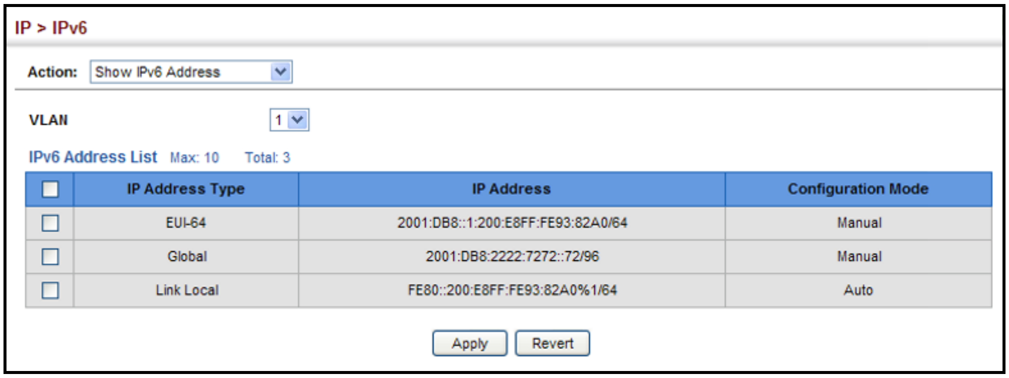
To show the configured IPv6 addresses:

1. Click IP, IPv6 Configuration.

2. Select Show IPv6 Address from the Action list.

3. Select a VLAN from the list.

**Figure 7: Showing Configured IPv6 Addresses**




## Showing the IPv6 Neighbor Cache

Use the IP > IPv6 Configuration (Show IPv6 Neighbor Cache) page to display the IPv6 addresses detected for neighbor devices.

### CLI References

■ "show ipv6 neighbors" on page 1102

### Parameters

These parameters are displayed in the web interface:

**Table 1: ShowIPv6 Neighbors** - display description

| Field | Description |
|---|---|
| IPv6 Address | IPv6 address of neighbor. |
| Age | The time since the address was verified as reachable (in seconds). A static entry is indicated by the value "Permanent." |
| Link-layer Address | Physical layer MAC address. |
| State | The following states are used for dynamic entries:<br>◆ Incomplete - Address resolution is being carried out on the entry. A neighbor solicitation message has been sent to the multicast address of the target, but it has not yet returned a neighbor advertisement message.<br>◆ Invalid - An invalidated mapping. Setting the state to invalid dis-associates the interface identified with this entry from the indicated mapping (RFC 4293).<br>◆ Reachable - Positive confirmation was received within the last ReachableTime interval that the forward path to the neighbor was functioning. While in Reachable state, the device takes no special action when sending packets.<br>◆ Stale - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. While in Stale state, the device takes no action until a packet is sent.<br>◆ Delay - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. A packet was sent within the last DELAY_FIRST_PROBE_TIME interval. If no reachability confirmation is received within this interval after entering the Delay state, the switch will send a neighbor solicitation message and change the state to Probe.<br>◆ Probe - A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer interval until confirmation of reachability is received.<br>◆ Unknown - Unknown state. |

**Table 1: ShowIPv6 Neighbors** - display description (Continued)

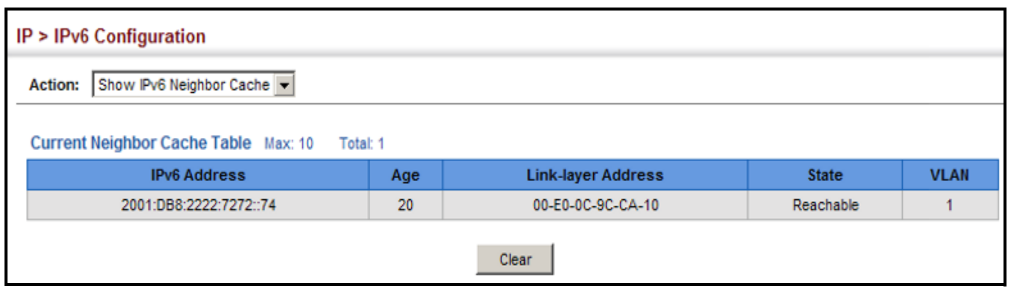
| Field | Description |
|---|---|
| | The following states are used for static entries:<br>◆ Incomplete - The interface for this entry is down.<br>◆ Permanent - Indicates a static entry.<br>◆ Reachable - The interface for this entry is up. Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache. |
| VLAN | VLAN interface from which the address was reached. |

### WEB INTERFACE

To show neighboring IPv6 devices:

1. Click IP, IPv6 Configuration.
2. Select Show IPv6 Neighbors from the Action list.

**Figure 8: Showing IPv6 Neighbors**




## Showing IPv6 Statistics

Use the IP > IPv6 Configuration (Show Statistics) page to display statistics about IPv6 traffic passing through this switch.

### CLI REFERENCES

■ "show ipv6 traffic" on page 1091

### COMMAND USAGE

This switch provides statistics for the following traffic types:

■ **IPv6** – The Internet Protocol for Version 6 addresses provides a mechanism for transmitting blocks of data (often called packets or frames) from a source to a destination, where these network devices (that is, hosts) are identified by fixed length addresses. The Internet Protocol also provides for fragmentation and reassembly of long packets, if necessary, for transmission through "small packet" networks.

■ **ICMPv6** – Internet Control Message Protocol for Version 6 addresses is a network layer protocol that transmits message packets to report errors in processing IPv6 packets. ICMP is therefore an integral part of the Internet Protocol. ICMP messages may be used to report various situations, such as when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route. ICMP is also used by routers to feed back information about more suitable routes (that is, the next hop router) to use for a specific destination.

- **UDP** – User Datagram Protocol provides a datagram mode of packet switched communications. It uses IP as the underlying transport mechanism, providing access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

### PARAMETERS

These parameters are displayed in the web interface:

**Table 2: Show IPv6 Statistics** - display description

| Field | Description |
|---|---|
| **IPv6 Statistics** | |
| *IPv6 Received* | |
| Total | The total number of input datagrams received by the interface, including those received in error. |
| Header Errors | The number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, IPv6 options, etc. |
| Too Big Errors | The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface. |
| No Routes | The number of input datagrams discarded because no route could be found to transmit them to their destination. |
| Address Errors | The number of input datagrams discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., ::0) and unsupported addresses (e.g., addresses with unallocated prefixes). For entities which are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address. |
| Unknown Protocols | The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams. |
| Truncated Packets | The number of input datagrams discarded because datagram frame didn't carry enough data. |
| Discards | The number of input IPv6 datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly. |
| Delivers | The total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams. |
| Reassembly Request Datagrams | The number of IPv6 fragments received which needed to be reassembled at this interface. Note that this counter is increment ed at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments. |
| Reassembled Succeeded | The number of IPv6 datagrams successfully reassembled. Note that this counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the fragments. |

**Table 2: Show IPv6 Statistics** - display description (Continued)

| Field | Description |
|---|---|
| Reassembled Failed | The number of failures detected by the IPv6 re-assembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received. This counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments. |
| *IPv6 Transmitted* | |
| Forwards Datagrams | The number of output datagrams which this entity received and forwarded to their final destinations. In entities which do not act as IPv6 routers, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route processing was successful. Note that for a successfully forwarded datagram the counter of the outgoing interface is incremented. |
| Requests | The total number of IPv6 datagrams which local IPv6 user-protocols (including ICMP) supplied to IPv6 in requests for transmission. Note that this counter does not include any datagrams counted in ipv6IfStatsOutForwDatagrams. |
| Discards | The number of output IPv6 datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipv6IfStatsOutForwDatagrams if any such packets met this (discretionary) discard criterion. |
| No Routes | The number of input datagrams discarded because no route could be found to transmit them to their destination. |
| Generated Fragments | The number of output datagram fragments that have been generated as a result of fragmentation at this output interface. |
| Fragment Succeeded | The number of IPv6 datagrams that have been successfully fragmented at this output interface. |
| Fragment Failed | The number of IPv6 datagrams that have been discarded because they needed to be fragmented at this output interface but could not be. |
| **ICMPv6 Statistics** | |
| *ICMPv6 received* | |
| Input | The total number of ICMP messages received by the interface which includes all those counted by ipv6IfIcmpInErrors. Note that this interface is the interface to which the ICMP messages were addressed which may not be necessarily the input interface for the messages. |
| Errors | The number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.). |
| Destination Unreachable Messages | The number of ICMP Destination Unreachable messages received by the interface. |
| Packet Too Big Messages | The number of ICMP Packet Too Big messages received by the interface. |
| Time Exceeded Messages | The number of ICMP Time Exceeded messages received by the interface. |
| Parameter Problem Messages | The number of ICMP Parameter Problem messages received by the interface. |
| Echo Request Messages | The number of ICMP Echo (request) messages received by the interface. |
| Echo Reply Messages | The number of ICMP Echo Reply messages received by the interface. |
| Router Solicit Messages | The number of ICMP Router Solicit messages received by the interface. |
| Router Advertisement Messages | The number of ICMP Router Advertisement messages received by the interface. |
| Neighbor Solicit Messages | The number of ICMP Neighbor Solicit messages received by the interface. |

**Table 2: Show IPv6 Statistics** - display description (Continued)

| Field | Description |
|---|---|
| Neighbor Advertisement Messages | The number of ICMP Neighbor Advertisement messages received by the interface. |
| Redirect Messages | The number of Redirect messages received by the interface. |
| Group Membership Query Messages | The number of ICMPv6 Group Membership Query messages received by the interface. |
| Group Membership Response Messages | The number of ICMPv6 Group Membership Response messages received by the interface. |
| Group Membership Reduction Messages | The number of ICMPv6 Group Membership Reduction messages received by the interface. |
| Multicast Listener Discovery Version 2 Reports | The number of MLDv2 reports received by the interface. |
| *ICMPv6 Transmitted* | |
| Output | The total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors. |
| Destination Unreachable Messages | The number of ICMP Destination Unreachable messages sent by the interface. |
| Packet Too Big Messages | The number of ICMP Packet Too Big messages sent by the interface. |
| Time Exceeded Messages | The number of ICMP Time Exceeded messages sent by the interface. |
| Echo Request Messages | The number of ICMP Echo (request) messages sent by the interface. |
| Echo Reply Messages | The number of ICMP Echo Reply messages sent by the interface. |
| Router Solicit Messages | The number of ICMP Router Solicitation messages sent by the interface. |
| Router Advertisement Messages | The number of ICMP Router Advertisement messages sent by the interface. |
| Neighbor Solicit Messages | The number of ICMP Neighbor Solicit messages sent by the interface. |
| Neighbor Advertisement Messages | The number of ICMP Router Advertisement messages sent by the interface. |
| Redirect Messages | The number of Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects. |
| Group Membership Query Messages | The number of ICMPv6 Group Membership Query messages sent by the interface. |
| Group Membership Response Messages | The number of ICMPv6 Group Membership Response messages sent. |
| Group Membership Reduction Messages | The number of ICMPv6 Group Membership Reduction messages sent. |
| Multicast Listener Discovery Version 2 Reports | The number of MLDv2 reports sent by the interface. |
| **UDP Statistics** | |
| Input | The total number of UDP datagrams delivered to UDP users. |
| No Port Errors | The total number of received UDP datagrams for which there was no application at the destination port. |
| Other Errors | The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port. |
| Output | The total number of UDP datagrams sent from this entity. |

**WEB INTERFACE**

To show the IPv6 statistics:

1. Click IP, IPv6 Configuration.
2. Select Show Statistics from the Action list.
3. Click IPv6, ICMPv6 or UDP.

**Figure 9: Showing IPv6 Statistics** (IPv6)

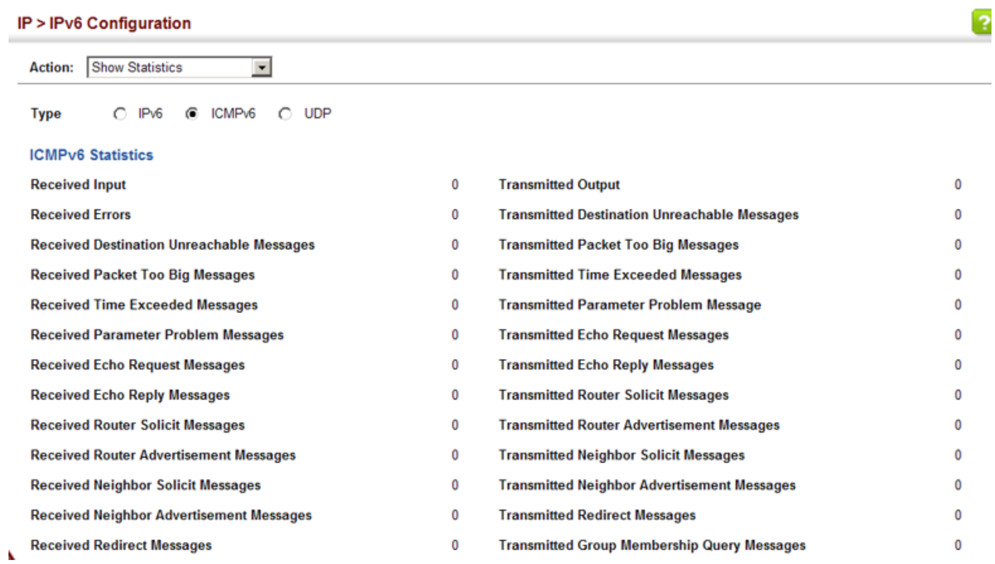


**Figure 10: Showing IPv6 Statistics** (ICMPv6)

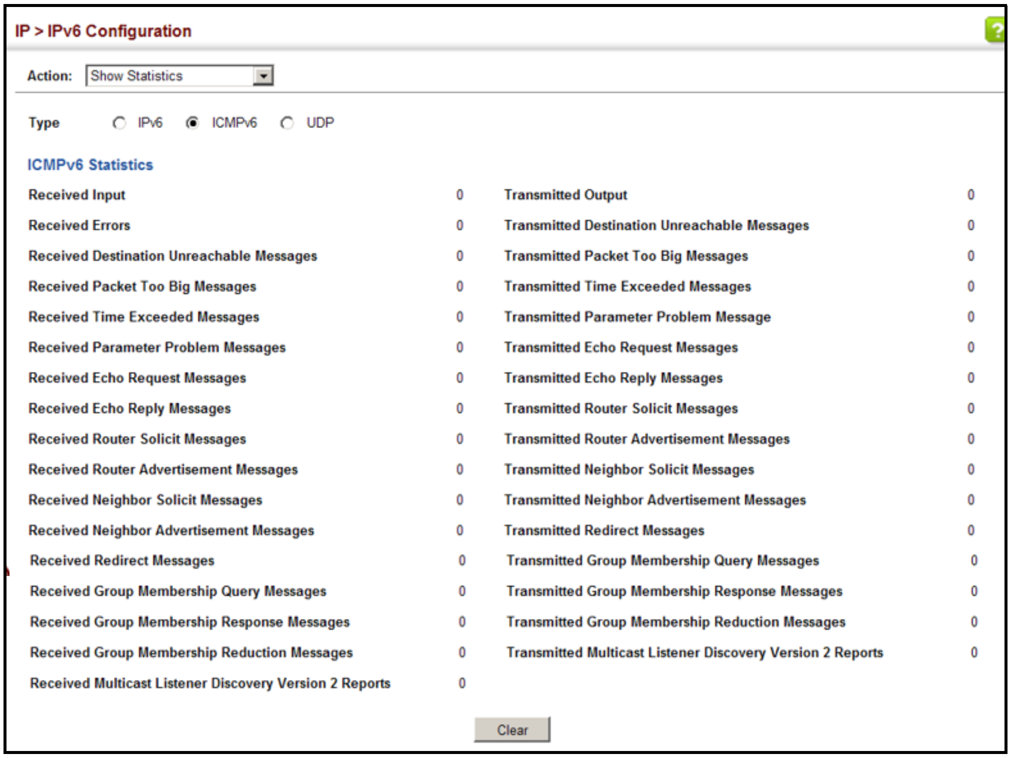
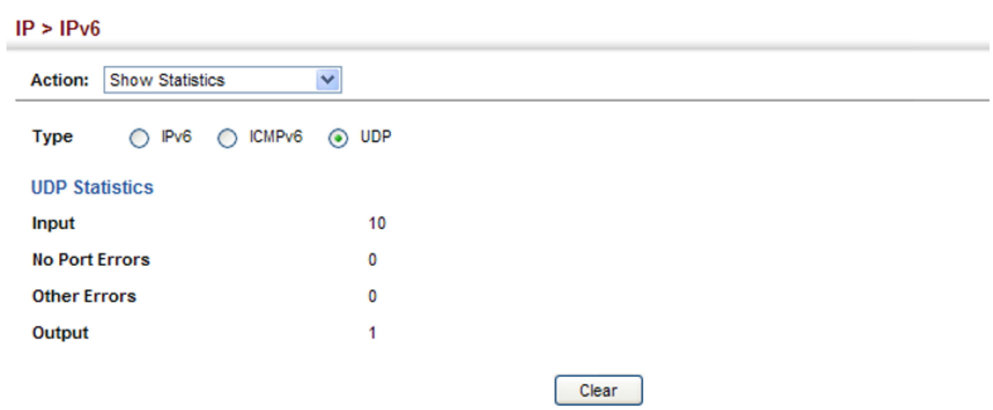



**Figure 11: Showing IPv6 Statistics** (UDP)



## Showing the MTU for Responding Destinations

Use the IP > IPv6 Configuration (Show MTU) page to display the maximum transmission unit (MTU) cache for destinations that have returned an ICMP packet-too-big message along with an acceptable MTU to this switch.

### CLI REFERENCES

■ "show ipv6 mtu" on page 1091

### PARAMETERS

These parameters are displayed in the web interface:

**Table 3: Show MTU** - display description

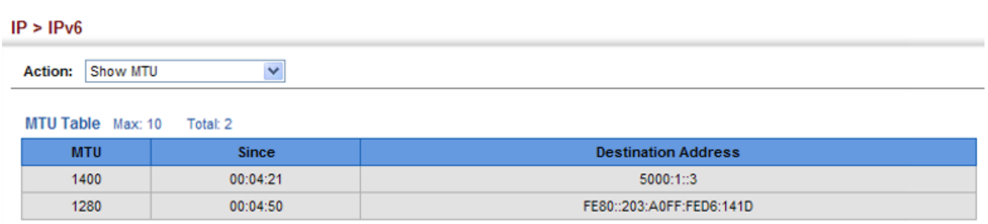
| Field | Description |
|---|---|
| MTU | Adjusted MTU contained in the ICMP packet-too-big message returned from this destination, and now used for all traffic sent along this path. |
| Since | Time since an ICMP packet-too-big message was received from this destination. |
| Destination Address | Address which sent an ICMP packet-too-big message. |

### WEB INTERFACE

To show the MTU reported from other devices:

1. Click IP, IPv6 Configuration.
2. Select Show MTU from the Action list.

**Figure 12: Showing Reported MTU Values**



# 18 GENERAL IP ROUTING

This chapter provides information on network functions including:

- Ping – Sends ping message to another node on the network.
- Trace – Sends ICMP echo request packets to another node on the network.
- Address Resolution Protocol – Describes how to configure ARP aging time, proxy ARP, or static addresses. Also shows how to display dynamic entries in the ARP cache.
- Static Routes – Configures static routes to other network segments.
- Routing Table – Displays routing entries learned through dynamic routing and statically configured entries.
- Equal-cost Multipath Routing – Configures the maximum number of equal-cost paths that can transmit traffic to the same destination

## OVERVIEW

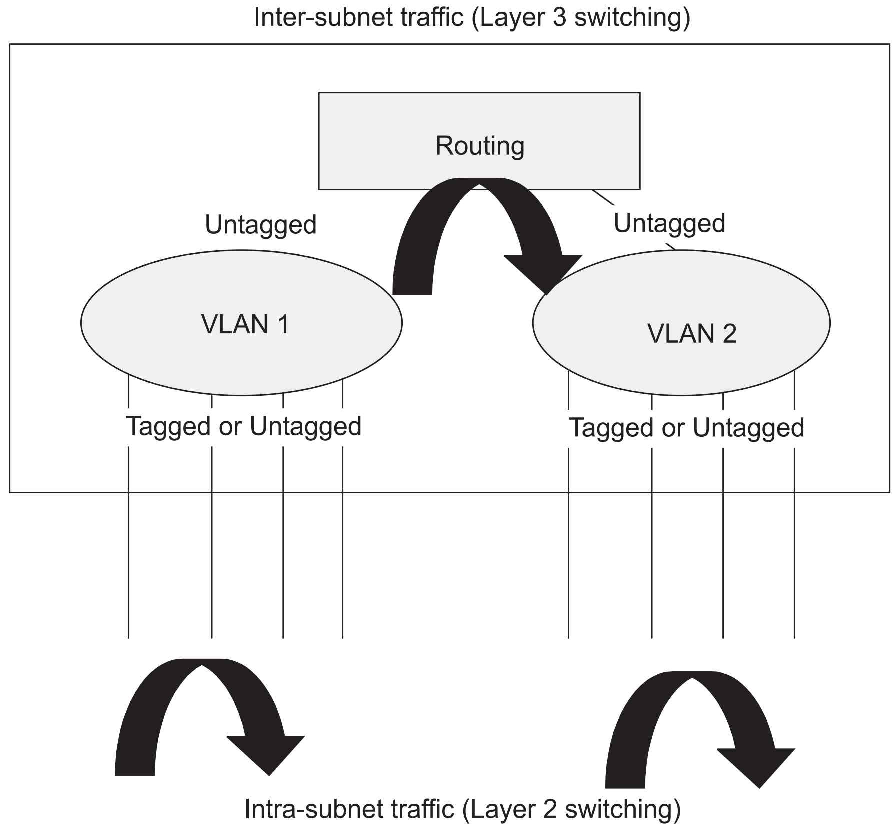
This switch supports IP routing and routing path management via static routing definitions (page 449) and dynamic routing protocols such as RIP, OSPF or OSPv3 (page 486 or 504, respectively). When IP routing is functioning, this switch acts as a wire-speed router, passing traffic between VLANs with different IP interfaces, and routing traffic to external IP networks. However, when the switch is first booted, default routing can only forward traffic between local IP interfaces. As with all traditional routers, static and dynamic routing functions must first be configured to work.

### Initial Configuration

By default, all ports belong to the same VLAN and the switch provides only Layer 2 functionality. To segment the attached network, first create VLANs for each unique user group or application traffic (page 140), assign all ports that belong to the same group to these VLANs (page 142), and then assign an IP interface to each VLAN (page 440). By separating the network into different VLANs, it can be partitioned into subnetworks that are disconnected at Layer 2. Network traffic within the same subnet is still switched using Layer 2 switching. And the VLANs can now be interconnected (as required) with Layer 3 switching.

Each VLAN represents a virtual interface to Layer 3. You just need to provide the network address for each virtual interface, and the traffic between different subnetworks will be routed by Layer 3 switching.

**Figure 1: Virtual Interfaces and Layer 3 Routing**




## IP ROUTING AND SWITCHING

IP Switching (or packet forwarding) encompasses tasks required to forward packets for both Layer 2 and Layer 3, as well as traditional routing. These functions include:

- Layer 2 forwarding (switching) based on the Layer 2 destination MAC address
- Layer 3 forwarding (routing):
  - Based on the Layer 3 destination address
  - Replacing destination/source MAC addresses for each hop
  - Incrementing the hop count
  - Decrementing the time-to-live
  - Verifying and recalculating the Layer 3 checksum

If the destination node is on the same subnetwork as the source network, then the packet can be transmitted directly without the help of a router. However, if the MAC address is not yet known to the switch, an Address Resolution Protocol (ARP) packet with the destination IP address is broadcast to get the destination MAC address from the destination node. The IP packet can then be sent directly with the destination MAC address.

If the destination belongs to a different subnet on this switch, the packet can be routed directly to the destination node. However, if the packet belongs to a subnet not included on this switch, then the packet should be sent to the next hop router (with the MAC address of the router itself used as the destination MAC address, and the destination IP address of the destination node). The router will then forward the packet to the destination node through the correct path. The router can also use the ARP protocol to find out the MAC address of the destination node of the next router as necessary.

**NOTE:** In order to perform IP switching, the switch should be recognized by other network nodes as an IP router, either by setting it as the default gateway or by redirection from another router via the ICMP process.

When the switch receives an IP packet addressed to its own MAC address, the packet follows the Layer 3 routing process. The destination IP address is checked against the Layer 3 address table. If the address is not already there, the switch broadcasts an ARP packet to all the ports on the destination VLAN to find out the destination MAC address. After the MAC address is discovered, the packet is reformatted and sent out to the destination. The reformat process includes decreasing the Time-To-Live (TTL) field of the IP header, recalculating the IP header checksum, and replacing the destination MAC address with either the MAC address of the destination node or that of the next hop router.

When another packet destined to the same node arrives, the destination MAC can be retrieved directly from the Layer 3 address table; the packet is then reformatted and sent out the destination port. IP switching can be done at wire-speed when the destination address entry is already in the Layer 3 address table.

If the switch determines that a frame must be routed, the route is calculated only during setup. Once the route has been determined, all packets in the current flow are simply switched or forwarded across the chosen path. This takes advantage of the high throughput and low latency of switching by enabling the traffic to bypass the routing engine once the path calculation has been performed.

## Routing Path Management

Routing Path Management involves the determination and updating of all the routing information required for packet forwarding, including:

- Handling routing protocols
- Updating the routing table
- Updating the Layer 3 switching database

## Routing Protocols

The switch supports both static and dynamic routing.

- Static routing requires routing information to be stored in the switch either manually or when a connection is set up by an application outside the switch.
- Dynamic routing uses a routing protocol to exchange routing information, calculate routing tables, and respond to changes in the status or loading of the network.

# CONFIGURING IP ROUTING INTERFACES

## Configuring Local and Remote Interfaces

Use the IP > General > Routing Interface page to configure routing interfaces for directly connected IPv4 subnets (see "Setting the Switch's IP Address (IP Version 4)" on page 417. Or use the IP > IPv6 Configuration pages to configure routing interfaces for directly connected IPv6 subnets (see "Setting the Switch's IP Address (IP Version 6)" on page 420).

If this router is directly connected to end node devices (or connected to end nodes through 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 prefix 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 segment that is connected to that interface, and allows you to send IP packets to or from the router.

You can specify the IP subnets connected directly to this router by manually assigning an IP address to each VLAN or using BOOTP or DHCP to dynamically assign an address. To specify IP subnets not directly connected to this router, you can either configure static routes (see page 449), or use the RIP or OSPF or OSPFv3 dynamic routing protocols (see page 485) to identify routes that lead to other interfaces by exchanging protocol messages with other routers on the network.

Once IP interfaces have been configured, the switch functions as a multilayer routing switch, operating at either Layer 2 or 3 as required. All IP packets are routed directly between local interfaces, or indirectly to remote interfaces using either static or dynamic routing. All other packets for non-IP protocols (for example, NetBuei, NetWare or AppleTalk) are switched based on MAC addresses).

To route traffic between remote IP interfaces, the switch should be recognized by other network nodes as an IP router, either by setting it to advertise itself as the default gateway or by redirection from another router via the ICMP process used by various routing protocols.

If the switch is configured to advertise itself as the default gateway, a routing protocol must still be used to determine the next hop router for any unknown destinations, i.e., packets that do not match any routing table entry. If another router is designated as the default gateway, then the switch will pass packets to this router for any unknown hosts or subnets.

To configure a default gateway for IPv4, use the static routing table as described on page 449, enter 0.0.0.0 for the IP address and subnet mask, and then specify this switch itself or another router as the gateway. To configure a gateway for IPv6, see "Configuring the IPv6 Default Gateway" on page 421.

## Using the Ping Function

Use the IP > General > Ping page to send ICMP echo request packets to another node on the network.

### CLI REFERENCES

■"ping" on page 1072

### PARAMETERS

These parameters are displayed in the web interface:

■**IP Address** – IP address of the host.

■**Probe Count** – Number of packets to send. (Range: 1-16)

■**Packet Size** – Number of bytes in a packet. (Range: 32-512 bytes)

The actual packet size will be eight bytes larger than the size specified because the switch adds header information.

### COMMAND USAGE

■Use the ping command to see if another site on the network can be reached.

■The following are some results of the **ping** command:

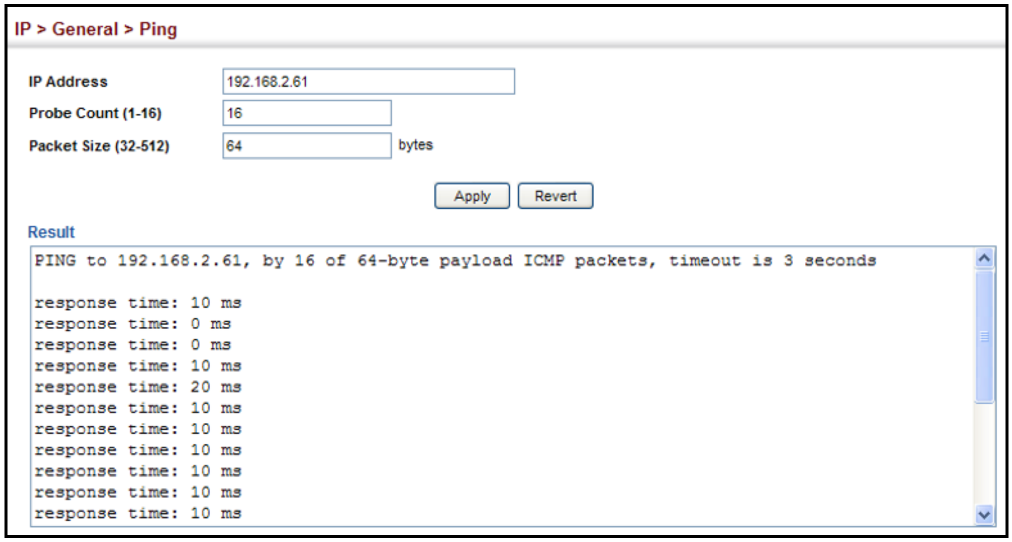
- ◆ *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.
- ◆ *Destination does not respond* - If the host does not respond, a “timeout” appears in ten seconds.
- ◆ *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
- ◆ *Network or host unreachable* - The gateway found no corresponding entry in the route table.

### WEB INTERFACE

To ping another device on the network:

1. Click IP, General, Ping.
2. Specify the target device and ping parameters.
3. Click Apply.

**Figure 2: Pinging a Network Device**




## Using the Trace Route Function

Use the IP > General > Trace Route page to show the route packets take to the specified destination.

### CLI REFERENCES

■"traceroute" on page 1071

### PARAMETERS

These parameters are displayed in the web interface:

■**Destination IP Address** – IP address of the host.

### COMMAND USAGE

■Use the trace route function to determine the path taken to reach a specified destination.

■A trace terminates when the destination responds, when the maximum timeout (TTL) is exceeded, or the maximum number of hops is exceeded.

■The trace route function first sends probe datagrams with the TTL value set at one. This causes the first router to discard the datagram and return an error message. The trace function then sends several probe messages at each subsequent TTL level and displays the round-trip time for each message. Not all devices respond correctly to probes by returning an “ICMP port unreachable” message. If the timer goes off before a response is returned, the trace function prints a series of asterisks and the “Request Timed Out” message. A long sequence of these messages, terminating only when the maximum timeout has been reached, may indicate this problem with the target device.

### WEB INTERFACE

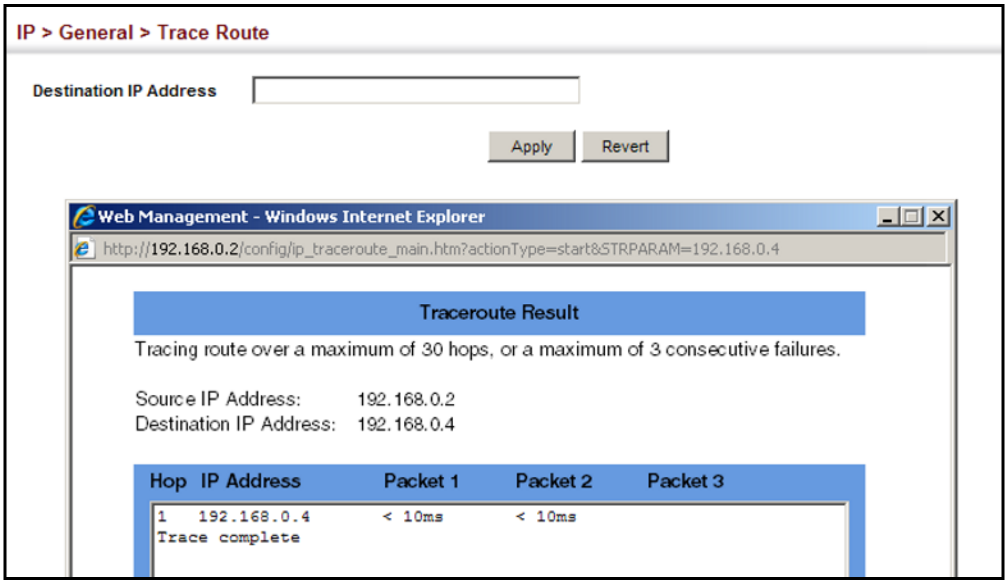
To trace the route to another device on the network:

**1.** Click IP, General, Trace Route.

2. Specify the target device.

3. Click Apply.

**Figure 3: Tracing the Route to a Network Device**




## ADDRESS RESOLUTION PROTOCOL

If IP routing is enabled (page 485), the router uses its routing tables to make routing decisions, and uses Address Resolution Protocol (ARP) to forward traffic from one hop to the next. ARP is used to map an IP address to a physical layer (i.e., MAC) address. When an IP frame is received by this router (or any standards-based router), it first looks up the MAC address corresponding to the destination IP address in the ARP cache. If the address is found, the router writes the MAC address into the appropriate field in the frame header, and forwards the frame on to the next hop. IP traffic passes along the path to its final destination in this way, with each routing device mapping the destination IP address to the MAC address of the next hop toward the recipient, until the packet is delivered to the final destination.

If there is no entry for an IP address in the ARP cache, the router will broadcast an ARP request packet to all devices on the network. The ARP request contains the following fields similar to that shown in this example:

**Table 1: Address Resolution Protocol**

| | |
|---|---|
| destination IP address | 10.1.0.19 |
| destination MAC address | ? |
| source IP address | 10.1.0.253 |
| source MAC address | 00-00-ab-cd-00-00 |

When devices receive this request, they discard it if their address does not match the destination IP address in the message. However, if it does match, they write their own hardware address into the destination MAC address field and send the message back to the source hardware address. When the source device receives a reply, it writes the destination IP address and corresponding MAC address into its cache, and forwards the IP traffic on to the next hop. As long as this entry has not timed out, the router will be able forward traffic directly to the next hop for this destination without having to broadcast another ARP request.

Also, if the switch receives a request for its own IP address, it will send back a response, and also cache the MAC of the source device's IP address.

## Basic ARP Configuration

Use the IP > ARP (Configure General) page to specify the timeout for ARP cache entries, or to enable Proxy ARP for specific VLAN interfaces.

### CLI References

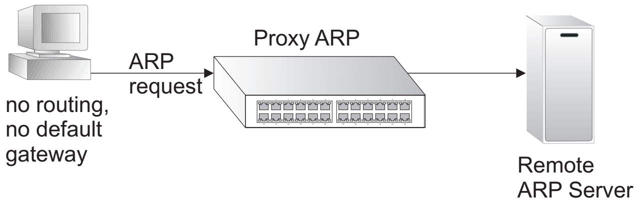
- "arp timeout" on page 1074
- "ip proxy-arp" on page 1075

### Command Usage

*Proxy ARP*

When a node in the attached subnetwork does not have routing or a default gateway configured, Proxy ARP can be used to forward ARP requests to a remote subnetwork. When the router receives an ARP request for a remote network and Proxy ARP is enabled, it determines if it has the best route to the remote network, and then answers the ARP request by sending its own MAC address to the requesting node. That node then sends traffic to the router, which in turn uses its own routing table to forward the traffic to the remote destination.

**Figure 4: Proxy ARP**




### Parameters

These parameters are displayed in the web interface:

- **Timeout** – Sets the aging time for dynamic entries in the ARP cache. (Range: 300 - 86400 seconds; Default: 1200 seconds or 20 minutes)

  The ARP aging timeout can be set for any configured VLAN.

  The aging time determines how long dynamic entries remain in the cache. If the timeout is too short, the router may tie up resources by repeating ARP requests for addresses recently flushed from the table.

  When a ARP entry expires, it is deleted from the cache and an ARP request packet is sent to re-establish the MAC address.

- **Proxy ARP** – Enables or disables Proxy ARP for specified VLAN interfaces, allowing a non-routing device to determine the MAC address of a host on another subnet or network. (Default: Disabled)

  End stations that require Proxy ARP must view the entire network as a single network. These nodes must therefore use a smaller subnet mask than that used by the router or other relevant network devices.

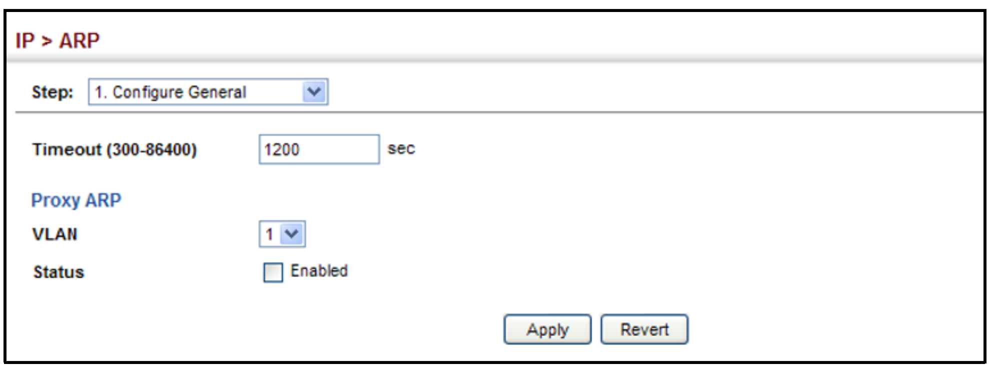
  Extensive use of Proxy ARP can degrade router performance because it may lead to increased ARP traffic and increased search time for larger ARP address tables.

### WEB INTERFACE

To configure the timeout for the ARP cache or to enable Proxy ARP for a VLAN (i.e., IP subnetwork):

1. Click IP, ARP.
2. Select Configure General from the Step List.
3. Set the timeout to a suitable value for the ARP cache, or enable Proxy ARP for subnetworks that do not have routing or a default gateway.
4. Click Apply.

**Figure 5: Configuring General Settings for ARP**




## Configuring Static ARP Addresses

For devices that do not respond to ARP requests or do not respond in a timely manner, traffic will be dropped because the IP address cannot be mapped to a physical address. If this occurs, use the IP > ARP (Configure Static Address – Add) page to manually map an IP address to the corresponding physical address in the ARP cache.

### CLI REFERENCES

- "arp" on page 1073

### COMMAND USAGE

- The ARP cache is used to map 32-bit IP addresses into 48-bit hardware (that is, Media Access Control) addresses. This cache includes entries for hosts and other routers on local network interfaces defined on this router.

- You can define up to 128 static entries in the ARP cache.

- A static entry may need to be used if there is no response to an ARP broadcast message. For example, some applications may not respond to ARP requests or the response arrives too late, causing network operations to time out.

- Static entries will not be aged out or deleted when power is reset. You can only remove a static entry via the configuration interface.

### PARAMETERS

These parameters are displayed in the web interface:

- **IP Address** – IP address statically mapped to a physical MAC address. (Valid IP addresses consist of four numbers, 0 to 255, separated by periods.)

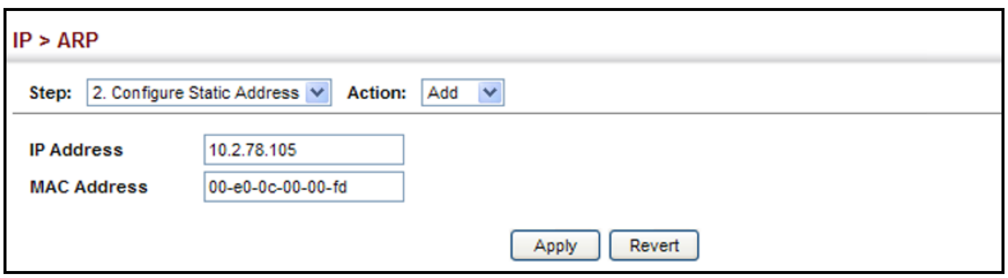
- **MAC Address** – MAC address statically mapped to the corresponding IP address. (Valid MAC addresses are hexadecimal numbers in the format: xx-xx-xx-xx-xx-xx)

### WEB INTERFACE

To map an IP address to the corresponding physical address in the ARP cache using the web interface:

1. Click IP, ARP.
2. Select Configure Static Address from the Step List.
3. Select Add from the Action List.
4. Enter the IP address and the corresponding MAC address.
5. Click Apply.

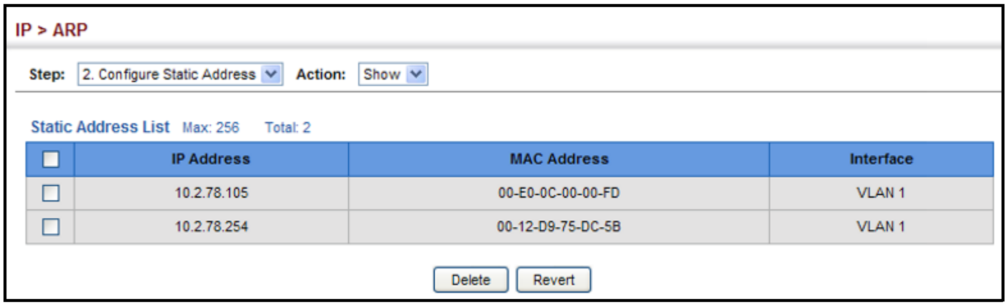
**Figure 6: Configuring Static ARP Entries**




To display static entries in the ARP cache:

1. Click IP, ARP.
2. Select Configure Static Address from the Step List.
3. Select Show from the Action List.

**Figure 7: Displaying Static ARP Entries**




## Displaying Dynamic or Local ARP Entries

The ARP cache contains static entries, and entries for local interfaces, including subnet, host, and broadcast addresses. However, most entries will be dynamically learned through replies to broadcast messages. Use the IP > ARP (Show Information) page to display dynamic or local entries in the ARP cache.

### CLI REFERENCES

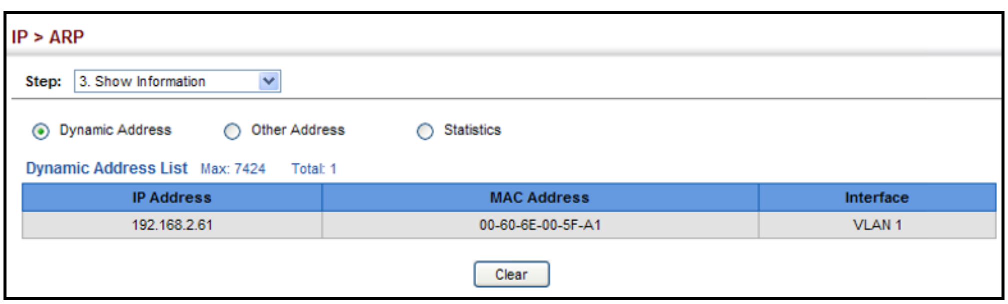
■"show arp" on page 1076

### WEB INTERFACE

To display all dynamic entries in the ARP cache:

1. Click IP, ARP.
2. Select Show Information from the Step List.
3. Click Dynamic Address.

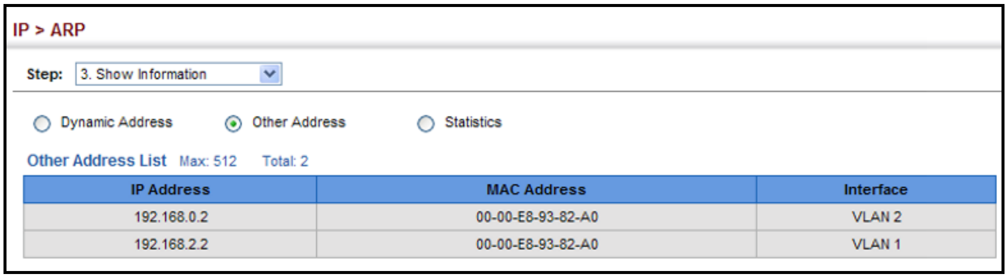
**Figure 8: Displaying Dynamic ARP Entries**




To display all local entries in the ARP cache:

1. Click IP, ARP.
2. Select Show Information from the Step List.
3. Click Other Address.

**Figure 9: Displaying Local ARP Entries**




## Displaying ARP Statistics

Use the IP > ARP (Show Information) page to display statistics for ARP messages crossing all interfaces on this router.

### CLI References

■ "show ip traffic" on page 1117

### Parameters

These parameters are displayed in the web interface:

**Table 2: ARP Statistics**

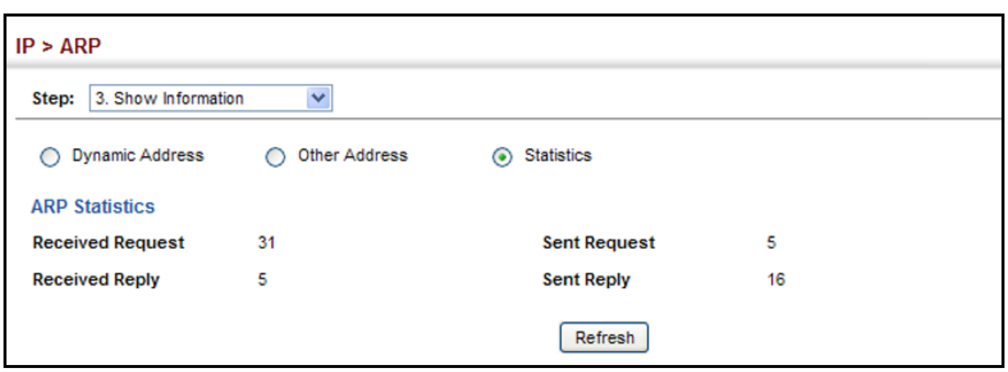
| Parameter | Description |
|---|---|
| Received Request | Number of ARP Request packets received by the router. |
| Received Reply | Number of ARP Reply packets received by the router. |
| Sent Request | Number of ARP Request packets sent by the router. |
| Sent Reply | Number of ARP Reply packets sent by the router. |

### Web Interface

To display ARP statistics:

1. Click IP, ARP.
2. Select Show Information from the Step List.
3. Click Statistics.

**Figure 10: Displaying ARP Statistics**



## CONFIGURING STATIC ROUTES

This router can dynamically configure routes to other network segments using dynamic routing protocols (i.e., RIP or OSPF). However, you can also manually enter static routes in the routing table using the IP > Routing > Static Routes (Add) page. Static routes may be required to access network segments where dynamic routing is not supported, or can be set to force the use of a specific route to a subnet, rather than using dynamic routing. Static routes do not automatically change in response to changes in network topology, so you should only configure a small number of stable routes to ensure network accessibility.

### CLI REFERENCES

■ "ip route" on page 1114

### COMMAND USAGE

■ Up to 512 static routes can be configured.

■ Up to eight equal-cost multipaths (ECMP) can be configured for static routing (see "Equal-cost Multipath Routing" on page 452).

■ If an administrative distance is defined for a static route, and the same destination can be reached through a dynamic route at a lower administration distance, then the dynamic route will be used.

■ If both static and dynamic paths have the same lowest cost, the first route stored in the routing table, either statically configured or dynamically learned via a routing protocol, will be used.

■ Static routes are included in RIP and OSPF updates periodically sent by the router if this feature is enabled by RIP or OSPF (see page 495 or 522, respectively).

### PARAMETERS

These parameters are displayed in the web interface:

■ **Destination IP Address** – IP address of the destination network, subnetwork, or host.

■ **Netmask / Prefix Length** – Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.

■ **Next Hop** – IP address of the next router hop used for this route.

■ **Distance** – An administrative distance indicating that this route can be overridden by dynamic routing information if the distance of the dynamic route is less than that configured for the static route. Note that the default administrative distances used by the dynamic unicast routing protocols is 110 for OSPF and 120 for RIP. (Range: 1-255, Default: 1)

### WEB INTERFACE

To configure static routes:

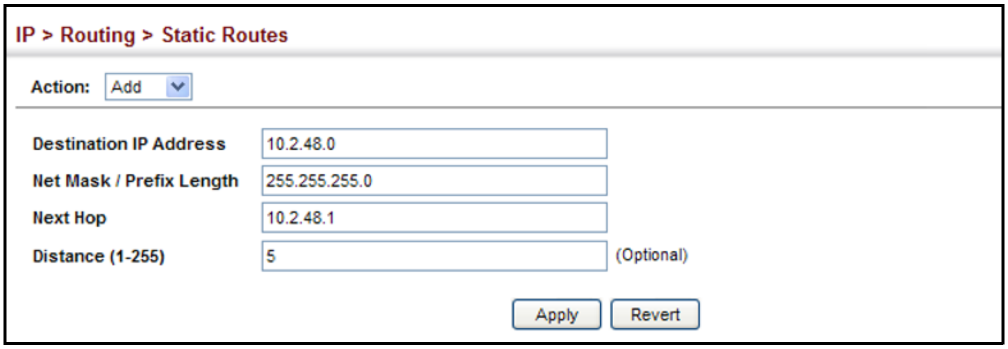
1. Click IP, Routing, Static Routes.

2. Select Add from the Action List.

3. Enter the destination address, subnet mask, and next hop router.

4. Click Apply.

**Figure 11: Configuring Static Routes**

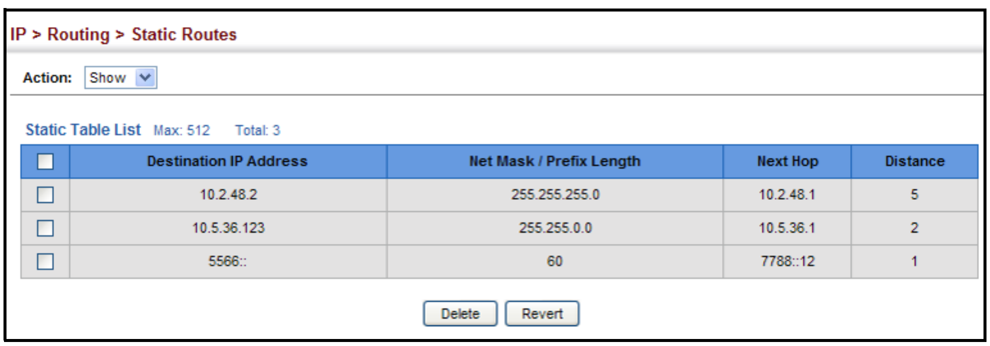



To display static routes:

1. Click IP, Routing, Static Routes.

2. Select Show from the Action List.

**Figure 12: Displaying Static Routes**




## DISPLAYING THE ROUTING TABLE

Use the IP > Routing > Routing Table page to display all routes that can be accessed via local network interfaces, through static routes, or through a dynamically learned route. If route information is available through more than one of these methods, the priority for route selection is local, static, and then dynamic (except when the distance parameter of a dynamic route is set to a value that makes its priority exceed that of a static route). Also note that the route for a local interface is not enabled (i.e., listed in the routing table) unless there is at least one active link connected to that interface.

### CLI REFERENCES

■ "show ip route" on page 1115

### Command Usage

- The Forwarding Information Base (FIB) contains information required to forward IP traffic. It contains the interface identifier and next hop information for each reachable destination network prefix based on the IP routing table. When routing or topology changes occur in the network, the routing table is updated, and those changes are immediately reflected in the FIB.

  The FIB is distinct from the routing table (or, Routing Information Base – RIB), which holds all routing information received from routing peers. The FIB contains unique paths only. It does not contain any secondary paths. A FIB entry consists of the minimum amount of information necessary to make a forwarding decision on a particular packet. The typical components within a FIB entry are a network prefix, a router (i.e., VLAN) interface, and next hop information.

- The Routing Table (and show ip route command) only displays routes which are currently accessible for forwarding. The router must be able to directly reach the next hop, so the VLAN interface associated with any dynamic or static route entry must be up. Note that routes currently not accessible for forwarding, may still be displayed by using the show ip route database command.

### Parameters

These parameters are displayed in the web interface:

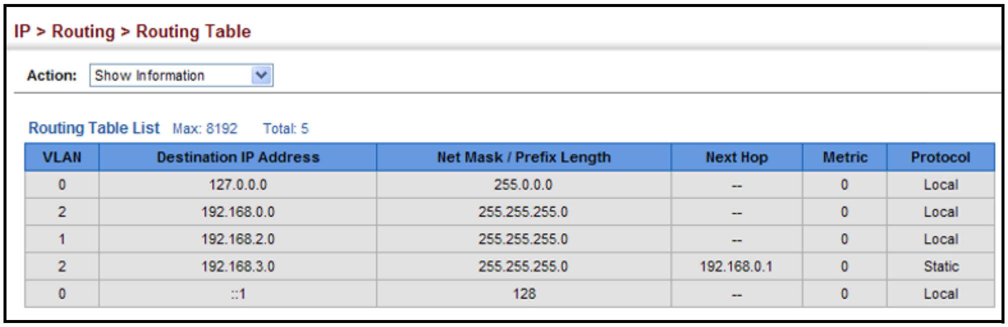
- **VLAN** – VLAN identifier (i.e., configure as a valid IP subnet).
- **Destination IP Address** – IP address of the destination network, subnetwork, or host. Note that the address 0.0.0.0 indicates the default gateway for this router.
- **Net Mask / Prefix Length** – Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **Next Hop** – The IP address of the next hop (or gateway) in this route.
- **Metric** – Cost for this interface.
- **Protocol** – The protocol which generated this route information. (Options: Local, Static, RIP, OSPF, Others)

### Web Interface

To display the routing table:

1. Click IP, Routing, Routing Table.
2. Select Show Information from the Action List.

**Figure 13: Displaying the Routing Table**



IP > Routing > Routing Table

Action: Show Information

Routing Table List Max: 8192 Total: 5

| VLAN | Destination IP Address | Net Mask / Prefix Length | Next Hop | Metric | Protocol |
|---|---|---|---|---|---|
| 0 | 127.0.0.0 | 255.0.0.0 | -- | 0 | Local |
| 2 | 192.168.0.0 | 255.255.255.0 | -- | 0 | Local |
| 1 | 192.168.2.0 | 255.255.255.0 | -- | 0 | Local |
| 2 | 192.168.3.0 | 255.255.255.0 | 192.168.0.1 | 0 | Static |
| 0 | ::1 | 128 | -- | 0 | Local |

## EQUAL-COST MULTIPATH ROUTING

Use the IP > Routing > Routing Table (Configure ECMP Number) page to configure the maximum number of equal-cost paths that can transmit traffic to the same destination. The Equal-cost Multipath routing algorithm is a technique that supports load sharing over multiple equal-cost paths for data passing to the same destination. Whenever multiple paths with equal path cost to the same destination are found in the routing table, the ECMP algorithm first checks if the cost is lower than that of any other entries in the routing table. If the cost is the lowest in the table, the switch will use up to eight of the paths with equal lowest cost to balance the traffic forwarded to the destination. ECMP uses either equal-cost multipaths manually configured in the static routing table, or equal-cost multipaths dynamically generated by the Open Shortest Path Algorithm (OSPF). In other words, it uses either static or OSPF entries, not both. Normal unicast routing simply selects the path to the destination that has the lowest cost. Multipath routing still selects the path with the lowest cost, but can forward traffic over multiple paths if they all have the same lowest cost. ECMP is enabled by default on the switch. If there is only one lowest cost path toward the destination, this path will be used to forward all traffic. If there is more than one lowest-cost path configured in the static routing table (see "Configuring Static Routes" on page 449), or dynamically generated by OSPFv2 (see "Configuring the Open Shortest Path First Protocol (Version 2)" on page 504), then up to 8 paths with the same lowest cost can be used to forward traffic to the destination.

### CLI REFERENCES

- "maximum-paths" on page 1115

### COMMAND USAGE

- ECMP only selects paths of the same protocol type. It cannot be applied to both static paths and dynamic paths at the same time for the same destination. If both static and dynamic paths have the same lowest cost, the static paths have precedence over dynamic paths.

- Each path toward the same destination with equal-cost takes up one entry in the routing table to record routing information. In other words, a route with 8 paths will take up 8 entries.

- The routing table can only have up to 8 equal-cost multipaths for static routing and 8 for dynamic routing for a common destination. However, the system supports up to 256 total ECMP entries in ASIC for fast switching, with any additional entries handled by software routing.

- When there are multiple paths toward the same destination with equal-cost, the system chooses one of these paths to forward each packet toward the destination by applying a load-splitting algorithm.

  A hash value is calculated based upon the source and destination IP fields of each packet as an indirect index to one of the multiple paths. Because the hash algorithm is calculated based upon the packet header information which can identify specific traffic flows, this technique minimizes the number of times a path is changed for individual flows. In general, path changes for individual flows will only occur when a path is added or removed from the multipath group.

### PARAMETERS

These parameters are displayed in the web interface:

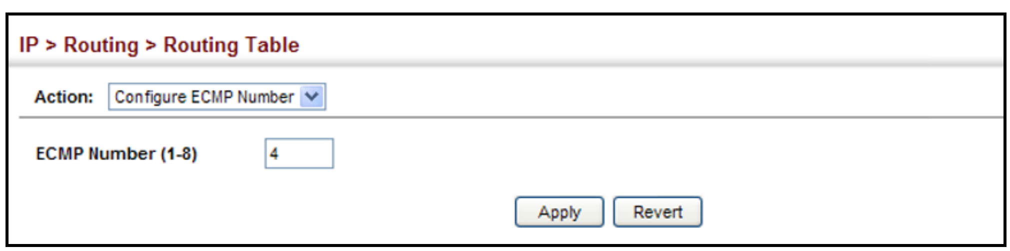
- **ECMP Number** – Sets the maximum number of equal-cost paths to the same destination that can be installed in the routing table. (Range: 1-8; Default: 4)

### WEB INTERFACE

To configure the maximum ECMP number:

1. Click IP, Routing, Routing Table.
2. Select Configure ECMP Number from the Action List.
3. Enter the maximum number of equal-cost paths used to route traffic to the same destination that are permitted on the switch.
4. Click Apply

**Figure 14: Setting the Maximum ECMP Number**



# 19 CONFIGURING ROUTER REDUNDANCY

Router redundancy protocols use a virtual IP address to support a primary router and multiple backup routers. The backup routers can be configured to take over the workload if the master router fails, or can also be configured to share the traffic load. The primary goal of router redundancy is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

This switch supports the Virtual Router Redundancy Protocol (VRRP). VRRP allows you to specify the interface of one of the routers participating in the virtual group as the address for the master virtual router, or to configure an arbitrary address for the virtual master router. VRRP then selects the backup routers based on the specified virtual router priority.

Router redundancy can be set up in any of the following configurations. These examples use the address of one of the participating routers as the master router. When the virtual router IP address is not a real address, the master router is selected based on priority. When the priority is the same on several competing routers, then the router with the highest IP address is selected as the master.

**Figure 1: Master Virtual Router with Backup Routers**

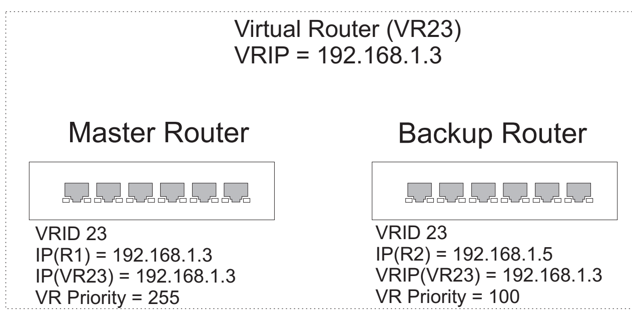



**Figure 2: Several Virtual Master Routers Using Backup Routers**

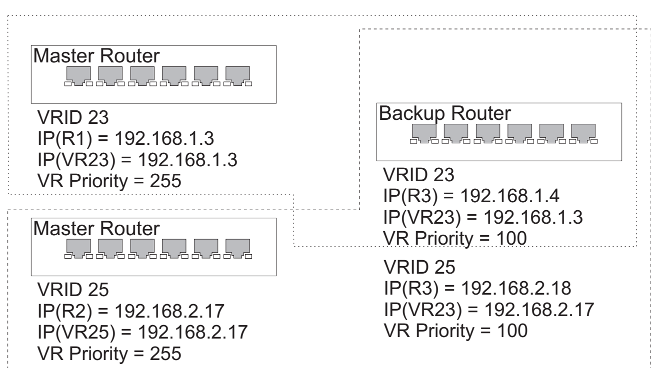
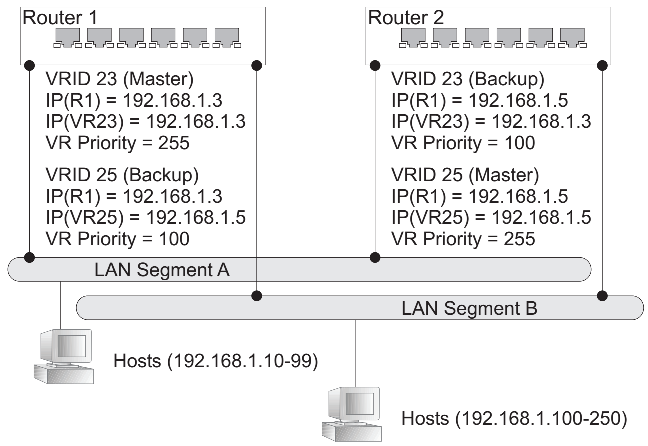


**Figure 3: Several Virtual Master Routers Configured for Mutual Backup and Load Sharing**




**NOTE:** Load sharing can be accomplished by assigning a subset of addresses to different host address pools using the DHCP server. (See "Configuring Address Pools" on page 476)

## CONFIGURING VRRP GROUPS

Use the IP > VRRP pages to configure VRRP. To configure VRRP groups, select an interface on each router in the group that will participate in the protocol as the master router or a backup router. To select a specific device as the master router, set the address of this interface as the virtual router address for the group. Now set the same virtual address and a priority on the backup routers, and configure an authentication string. You can also enable the preempt feature which allows a router to take over as the master router when it comes on line if it has a higher priority than the currently active master router.

### CLI REFERENCES

- "VRRP Commands" on page 1057

### COMMAND USAGE

*Address Assignment –*

- To designate a specific router as the VRRP master, the IP address assigned to the virtual router must already be configured on the router that will become the Owner of the group address. In other words, the IP address for the virtual router exists on one, and only one, router in the virtual router group, and the network mask for the virtual router address is derived from the Owner. The Owner will also assume the role of the Master virtual router in the group.

- If a virtual address is assigned to the group which does not exist on any of the group members, then the master router is selected based on priority. In cases where the configured priority is the same on several group members, then the master router with the highest IP address is selected from this group.

- If you have multiple secondary addresses configured on the current VLAN interface, you can add any of these addresses to the virtual router group.

- The interfaces of all routers participating in a virtual router group must be within the same IP subnet.

- VRRP creates a virtual MAC address for the master router based on a standard prefix, with the last octet equal to the group ID. When a backup router takes over as the master, it continues to forward traffic addressed to this virtual MAC address. However, the backup router cannot reply to ICMP pings sent to addresses associated with the virtual group because the IP address owner is off line.

*Virtual Router Priority –*

- The Owner of the virtual IP address is automatically assigned the highest possible virtual router priority of 255. The backup router with the highest priority will become the master router if the current master fails. However, because the priority of the virtual IP address Owner is the highest, the original master router will always become the active master router when it recovers.

- If two or more routers are configured with the same VRRP priority, the router with the higher IP address is elected as the new master router if the current master fails.

*Preempting the Acting Master –*

- The virtual IP Owner has the highest priority, so no other router can preempt it, and it will always resume control as the master virtual router when it comes back on line. The preempt function only allows a backup router to take over from a master router if no router in the group is the virtual IP owner, or from another backup router that is temporarily acting as the group master. If preemption is enabled and this router has a higher priority than the current acting master when it comes on line, it will take over as the acting group master.

- You can add a delay to the preempt function to give additional time to receive an advertisement message from the current master before taking control. If the router attempting to become the master has just come on line, this delay also gives it time to gather information for its routing table before actually preempting the currently active master router.

### PARAMETERS

These parameters are displayed in the web interface:

*Adding a VRRP Group*

- **VRID** – VRRP group identifier. (Range: 1-255)

- **VLAN** – ID of a VLAN configured with an IP interface. (Range: 1-4093; Default: 1)

*Adding a Virtual IP Address*

- **VLAN ID** – ID of a VLAN configured with an IP interface. (Range: 1-4093)

- **VRID** – VRRP group identifier. (Range: 1-255)

- **IP Address** – Virtual IP address for this group.

  Use the IP address of a real interface on this router to make it the master virtual router for the group. Otherwise, use the virtual address for an existing group to make it a backup router, or to compete as the master based on configured priority if no other members are set as the owner of the group address.

*Configuring Detailed Settings*

- **VLAN ID** – VLAN configured with an IP interface. (Range: 1-4093)

- **VRID** – VRRP group identifier. (Range: 1-255)

- **Advertisement Interval** – Interval at which the master virtual router sends advertisements communicating its state as the master. (Range: 1-255 seconds; Default: 1 second)

  VRRP advertisements from the current master virtual router include information about its priority and current state as the master.

  VRRP advertisements are sent to the multicast address 224.0.0.8. Using a multicast address reduces the amount of traffic that has to be processed by network devices that are not part of the designated VRRP group.

  If the master router stops sending advertisements, backup routers will bid to become the master router based on priority. The dead interval before attempting to take over as the master is three times the hello interval plus half a second.

- **Priority** – The priority of this router in a VRRP group. (Range: 1-254; Default: 100)

  - The priority for the VRRP group address owner is automatically set to 255.
  - The priority for backup routers is used to determine which router will take over as the acting master router if the current master fails.

- **Preempt Mode** – Allows a backup router to take over as the master virtual router if it has a higher priority than the acting master virtual router (i.e., a master router that is not the group's address owner, or another backup router that has taken over from the previous master). (Default: Enabled)

- **Preempt Delay Time** – Time to wait before issuing a claim to become the master. (Range: 0-120 seconds; 0 seconds)

- **Authentication Mode** – Authentication mode used to verify VRRP packets received from other routers. (Options: None, Simple Text; Default: None)

  If simple text authentication is selected, then you must also enter an authentication string.

  All routers in the same VRRP group must be set to the same authentication mode, and be configured with the same authentication string.

  Plain text authentication does not provide any real security. It is supported only to prevent a misconfigured router from participating in VRRP.

- **Authentication String** – Key used to authenticate VRRP packets received from other routers. (Range: 1-8 alphanumeric characters)

When a VRRP packet is received from another router in the group, its authentication string is compared to the string configured on this router. If the strings match, the message is accepted. Otherwise, the packet is discarded.

- **State** – VRRP router role. (Values: Master, Backup)
- **Virtual MAC Address** – Virtual MAC address for this group.
- **Master Router** – The primary router servicing this group.
- **Master Priority** – The priority of the master router.
- **Master Advertisement Interval** – The interval at which the master router sends messages advertising itself as the group master.
- **Master Down Interval** – If no advertisement message is received from the master router after this interval, backup routers will assume that the master is dead, and will start bidding to become the group master.

### WEB INTERFACE

To configure VRRP:

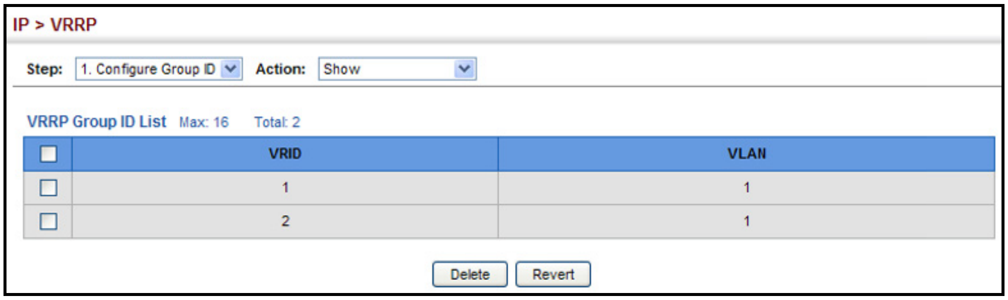
1. Click IP, VRRP.
2. Select Configure Group ID from the Step List.
3. Select Add from the Action List.
4. Enter the VRID group number, and select the VLAN (i.e., IP subnet) which is to be serviced by this group.
5. Click Apply.

**Figure 4: Configuring the VRRP Group ID**


To show the configured VRRP groups:

1. Click IP, VRRP.
2. Select Configure Group ID from the Step List.
3. Select Show from the Action List.

**Figure 5: Showing Configured VRRP Groups**




To configure the virtual router address for a VRRP group:

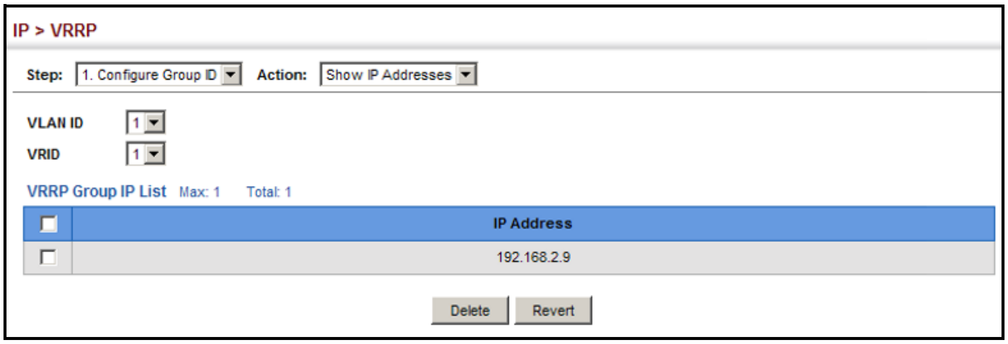
1. Click IP, VRRP.
2. Select Configure Group ID from the Step List.
3. Select Add IP Address from the Action List.
4. Select a VLAN, a VRRP group identifier, and enter the IP address for the virtual router.
5. Click Apply.

**Figure 6: Setting the Virtual Router Address for a VRRP Group**


To show the virtual IP address assigned to a VRRP group:

1. Click IP, VRRP.
2. Select Configure Group ID from the Step List.
3. Select Show IP Addresses from the Action List.
4. Select a VLAN, and a VRRP group identifier.

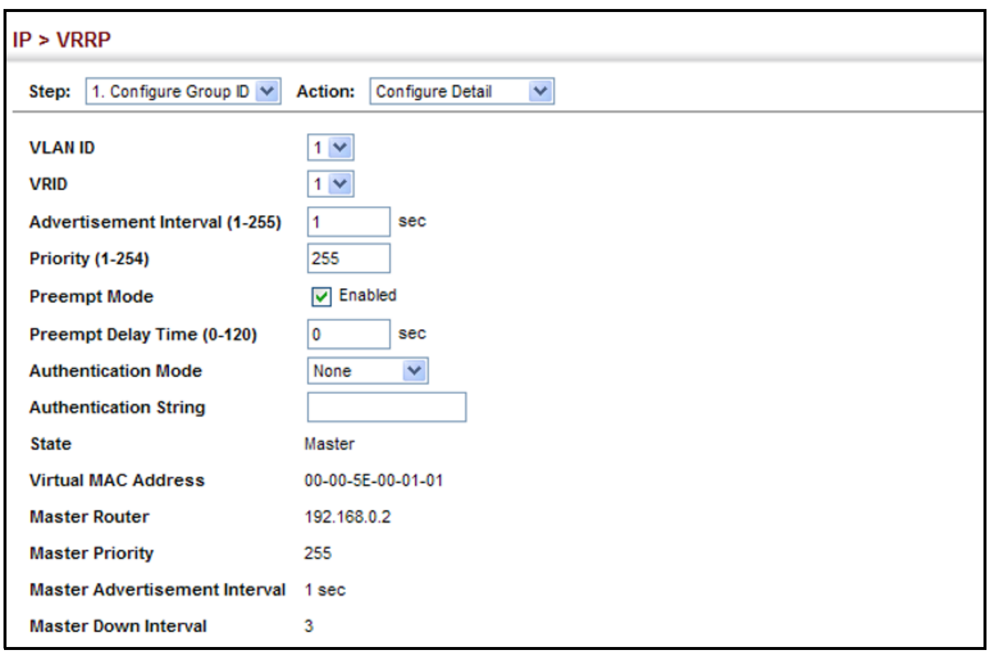
**Figure 7: Showing the Virtual Addresses Assigned to VRRP Groups**




To configure detailed settings for a VRRP group:

1. Click IP, VRRP.
2. Select Configure Group ID from the Step List.
3. Select Configure Detail from the Action List.
4. Select a VRRP group identifier, and set any of the VRRP protocol parameters as required.
5. Click Apply.

**Figure 8: Configuring Detailed Settings for a VRRP Group**



## DISPLAYING VRRP GLOBAL STATISTICS

Use the IP > VRRP (Show Statistics – Global Statistics) page to display counters for errors found in VRRP protocol packets.

### CLI REFERENCES

■ "show vrrp router counters" on page 1066

### PARAMETERS

These parameters are displayed in the web interface:

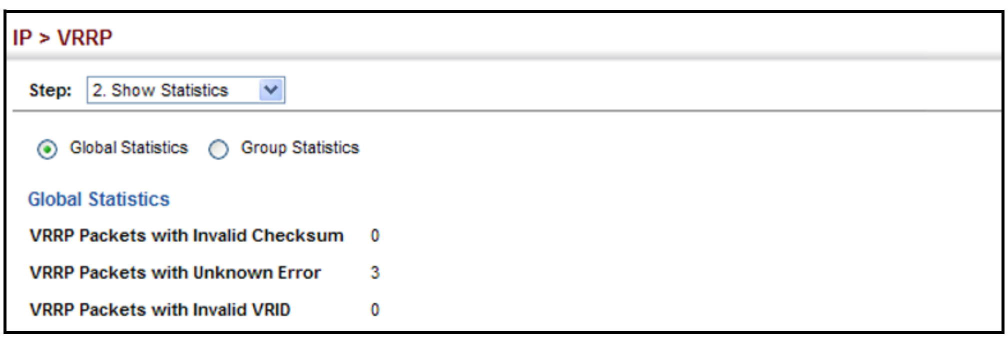
- **VRRP Packets with Invalid Checksum** – The total number of VRRP packets received with an invalid VRRP checksum value.
- **VRRP Packets with Unknown Error** – The total number of VRRP packets received with an unknown or unsupported version number.
- **VRRP Packets with Invalid VRID** – The total number of VRRP packets received with an invalid VRID for this virtual router.

### WEB INTERFACE

To show counters for errors found in VRRP protocol packets:

1. Click IP, VRRP.
2. Select Show Statistics from the Step List.
3. Click Global Statistics.

**Figure 9: Showing Counters for Errors Found in VRRP Packets**




## DISPLAYING VRRP GROUP STATISTICS

Use the IP > VRRP (Show Statistics – Group Statistics) page to display counters for VRRP protocol events and errors that have occurred on a specific VRRP interface.

### CLI REFERENCES

■ "show vrrp interface counters" on page 1065

### PARAMETERS

These parameters are displayed in the web interface:

- **VLAN ID** – VLAN configured with an IP interface. (Range: 1-4093)
- **VRID** – VRRP group identifier. (Range: 1-255)

The following statistics are displayed in the web interface:

**Table 1: VRRP Group Statistics**

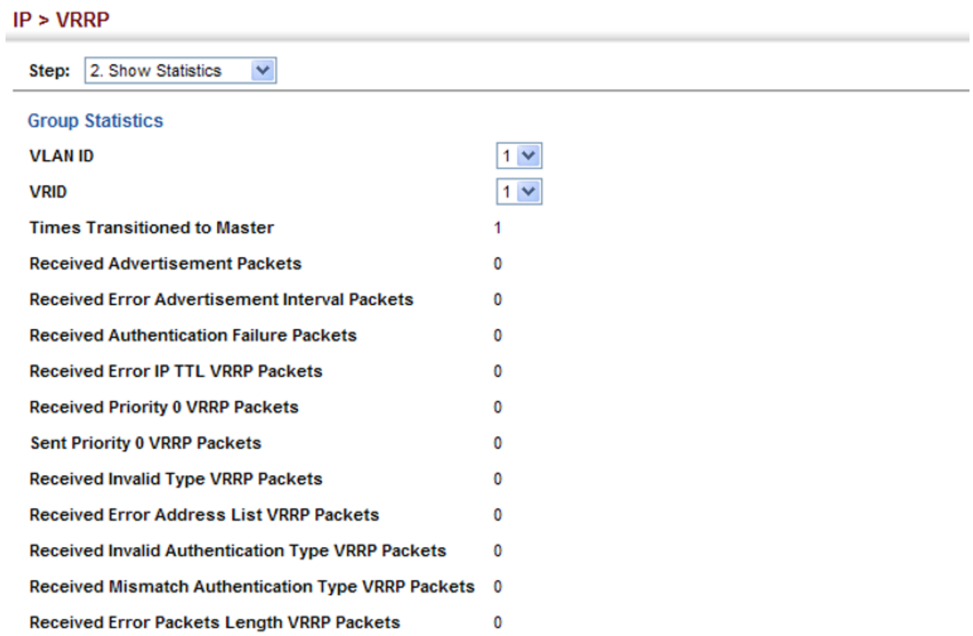
| Parameter | Description |
|---|---|
| Times Transitioned to Master | Number of times this router has transitioned to master. |
| Received Advertisement Packets | Number of VRRP advertisements received by this router. |
| Received Error Advertisement Interval Packets | Number of VRRP advertisements received for which the advertisement interval is different from the one configured for the local virtual router. |
| Received Authentication Failure Packets | Number of VRRP packets received that do not pass the authentication check. |
| Received Error IP TTL VRRP Packets | Number of VRRP packets received by the virtual router with IP TTL (Time-To-Live) not equal to 255. |
| Received Priority 0 VRRP Packets | Number of VRRP packets received by the virtual router with priority set to 0. |
| Sent Priority 0 VRRP Packets | Number of VRRP packets sent by the virtual router with priority set to 0. A priority value of zero indicates that the group master has stopped participating in VRRP, and is used to quickly transition a backup unit to master mode without having to wait for the master to time out. |
| Received Invalid Type VRRP Packets | Number of VRRP packets received by the virtual router with an invalid value in the “type” field. |
| Received Error Address List VRRP Packets | Number of packets received for which the address list does not match the locally configured list for the virtual router. |
| Received Invalid Authentication Type VRRP Packets | Number of packets received with an unknown authentication type. |
| Received Mismatch Authentication Type VRRP Packets | Number of packets received with “Auth Type” not equal to the locally configured authentication method. |
| Received Error Packets Length VRRP Packets | Number of packets received with a packet length less than the length of the VRRP header. |

### WEB INTERFACE

To show counters for VRRP protocol events and errors that occurred on a specific VRRP interface:

1. Click IP, VRRP.
2. Select Show Statistics from the Step List.
3. Click Group Statistics.

**Figure 10: Showing Counters for Errors Found in a VRRP Group**



# 20 IP SERVICES

This chapter describes the following IP services:

- DNS – Configures default domain names, identifies servers to use for dynamic lookup, and shows how to configure static entries.
- DHCP Client – Specifies the DHCP client identifier for an interface.
- DHCP Relay – Enables DHCP relay service, and defines the servers to which client requests are forwarded.
- DHCP Server – Configures address to be allocated to networks or specific hosts.
- UDP Helper – Configures the switch to forward UDP broadcast packets originating from host applications to another part of the network.

## DOMAIN NAME SERVICE

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 Service Parameters

Use the IP Service > DNS - General (Configure Global) page to enable domain lookup and set the default domain name.

#### CLI REFERENCES

- "ip domain-lookup" on page 1032
- "ip domain-name" on page 1033

#### COMMAND USAGE

- To enable DNS service on this switch, enable domain lookup status, and configure one or more name servers (see "Configuring a List of Name Servers" on page 468).

### PARAMETERS

These parameters are displayed in the web interface:

- **Domain Lookup** – Enables DNS host name-to-address translation. (Default: Disabled)
- **Default Domain Name** – Defines the default domain name appended to incomplete host names. Do not include the initial dot that separates the host name from the domain name.
  (Range: 1-127 alphanumeric characters)

### WEB INTERFACE

To configure general settings for DNS:

1. Click IP Service, DNS.
2. Select Configure Global from the Action list.
3. Enable domain lookup, and set the default domain name.
4. Click Apply.

**Figure 1: Configuring General Settings for DNS**


## Configuring a List of Domain Names

Use the IP Service > DNS - General (Add Domain Name) page to configure a list of domain names to be tried in sequential order.

### CLI REFERENCES

- "ip domain-list" on page 1031
- "show dns" on page 1037

### COMMAND USAGE

- Use this page to define 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).
- If there is no domain list, the default domain name is used (see "Configuring General DNS Service Parameters" on page 465). If there is a domain list, the system will search it for a corresponding entry. If none is found, it will use the default domain name.

■ When an incomplete host name is received by the DNS service on this switch and a domain name list has been specified, the switch will work through the domain list, appending each domain name in the list to the host name, and checking with the specified name servers for a match (see "Configuring a List of Name Servers" on page 468).

### PARAMETERS

These parameters are displayed in the web interface:

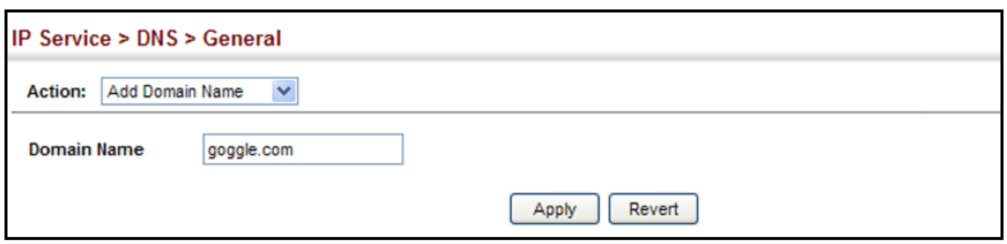
**Domain Name** – Name of the host. Do not include the initial dot that separates the host name from the domain name.
(Range: 1-68 characters)

### WEB INTERFACE

To create a list domain names:

1. Click IP Service, DNS.
2. Select Add Domain Name from the Action list.
3. Enter one domain name at a time.
4. Click Apply.

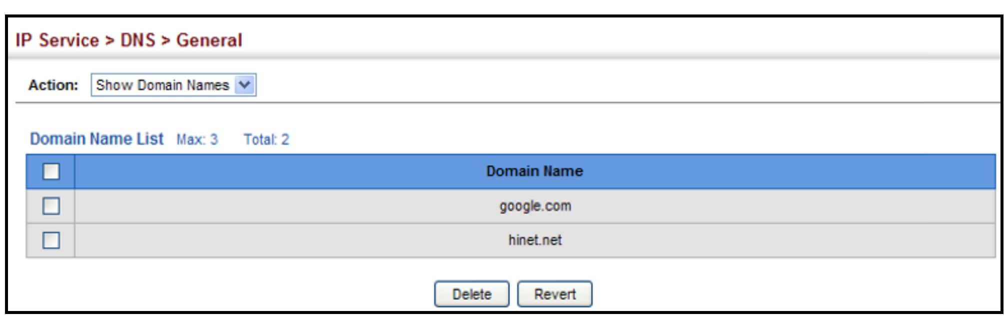
**Figure 2: Configuring a List of Domain Names for DNS**




To show the list domain names:

1. Click IP Service, DNS.
2. Select Show Domain Names from the Action list.

**Figure 3: Showing the List of Domain Names for DNS**



## Configuring a List of Name Servers

Use the IP Service > DNS - General (Add Name Server) page to configure a list of name servers to be tried in sequential order.

### CLI REFERENCES

- "ip name-server" on page 1034
- "show dns" on page 1037

### COMMAND USAGE

- To enable DNS service on this switch, configure one or more name servers, and enable domain lookup status (see "Configuring General DNS Service Parameters" on page 465).
- 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.
- If all name servers are deleted, DNS will automatically be disabled. This is done by disabling the domain lookup status.

### PARAMETERS

These parameters are displayed in the web interface:

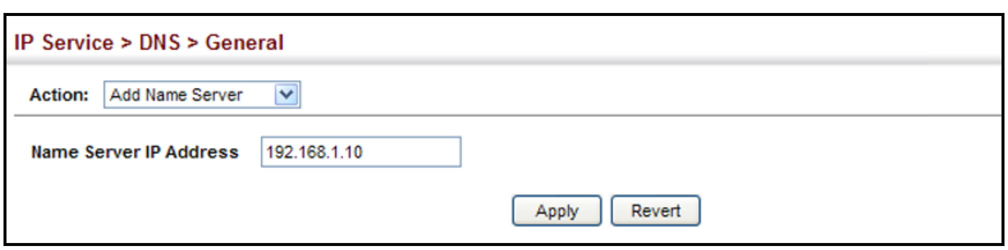
**Name Server IP Address** – Specifies the address of a domain name server to use for name-to-address resolution. Up to six IP addresses can be added to the name server list.

### WEB INTERFACE

To create a list name servers:

1. Click IP Service, DNS.
2. Select Add Name Server from the Action list.
3. Enter one name server at a time.
4. Click Apply.

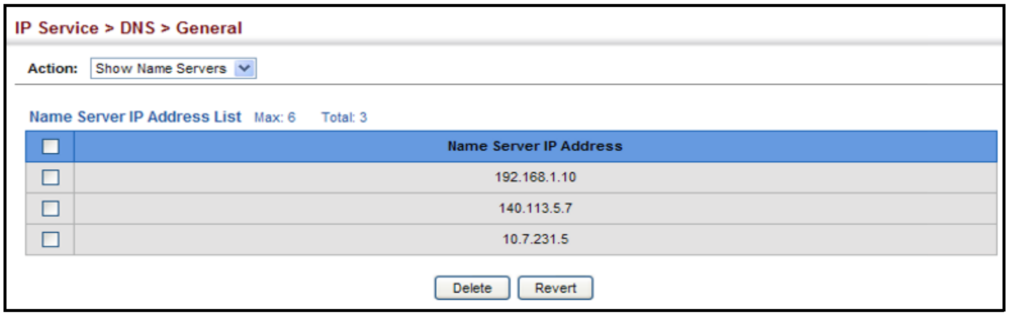
**Figure 4: Configuring a List of Name Servers for DNS**




To show the list name servers:

1. Click IP Service, DNS.
2. Select Show Name Servers from the Action list.

**Figure 5: Showing the List of Name Servers for DNS**




## Configuring Static DNS Host to Address Entries

Use the IP Service > DNS - Static Host Table (Add) page to manually configure static entries in the DNS table that are used to map domain names to IP addresses.

### CLI REFERENCES

■"ip host" on page 1034

■"show hosts" on page 1038

### 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.

### PARAMETERS

These parameters are displayed in the web interface:

■**Host Name** – Name of a host device that is mapped to one or more IP addresses. (Range: 1-127 characters)

■**IP Address** – Internet address(es) associated with a host name.

### WEB INTERFACE

To configure static entries in the DNS table:

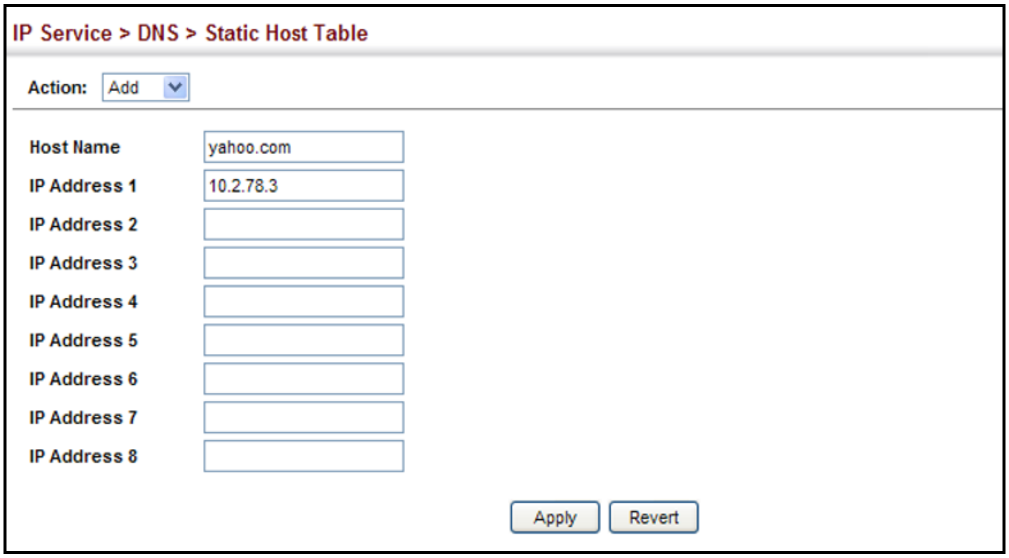
**1.** Click IP Service, DNS, Static Host Table.

**2.** Select Add from the Action list.

**3.** Enter a host name and the corresponding address.

**4.** Click Apply.

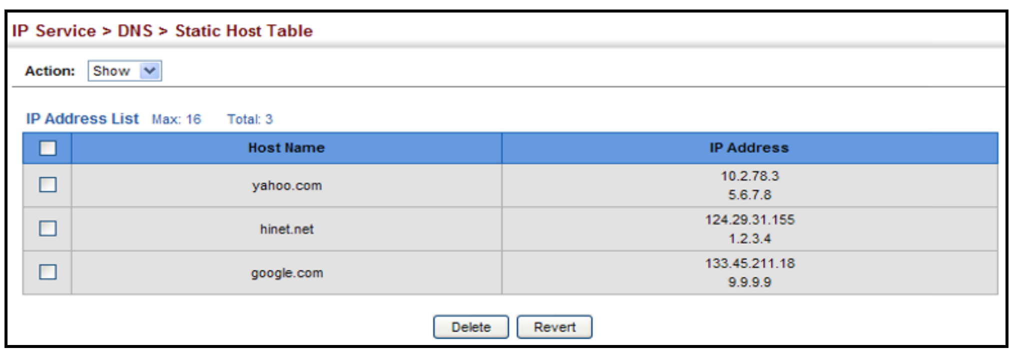
**Figure 6: Configuring Static Entries in the DNS Table**




To show static entries in the DNS table:

1. Click IP Service, DNS, Static Host Table.
2. Select Show from the Action list.

**Figure 7: Showing Static Entries in the DNS Table**




## Displaying the DNS Cache

Use the IP Service > DNS - Cache page to display entries in the DNS cache that have been learned via the designated name servers.

### CLI References

- "show dns cache" on page 1037

### 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 via information returned from a name server, a DNS client can try each address in succession, until it establishes a connection with the target device.

### PARAMETERS

These parameters are displayed in the web interface:

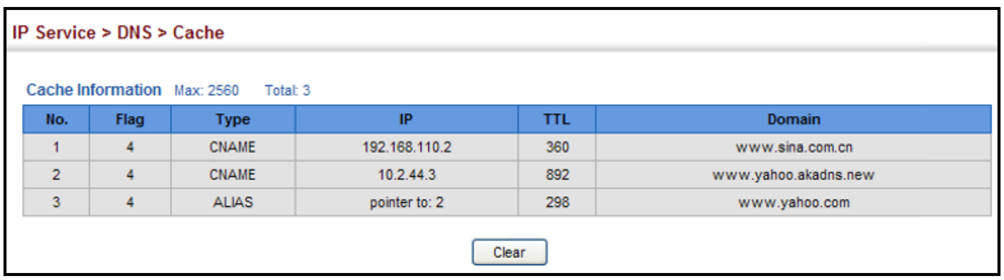
- **No.** – The entry number for each resource record.
- **Flag** – The flag is always “4” indicating a cache entry and therefore unreliable.
- **Type** – This field includes CNAME which specifies the host address for the owner, and ALIAS which specifies an alias.
- **IP** – The IP address associated with this record.
- **TTL** – The time to live reported by the name server.
- **Domain** – The domain name associated with this record.

### WEB INTERFACE

To display entries in the DNS cache:

1. Click IP Service, DNS, Cache.

**Figure 8: Showing Entries in the DNS Cache**




## DYNAMIC HOST CONFIGURATION PROTOCOL

Dynamic Host Configuration Protocol (DHCP) can dynamically allocate an IP address and other configuration information to network clients when they boot up. If a subnet does not already include a BOOTP or DHCP server, you can relay DHCP client requests to a DHCP server on another subnet, or configure the DHCP server on this switch to support that subnet.

When configuring the DHCP server on this switch, you can configure an address pool for each unique IP interface, or manually assign a static IP address to clients based on their hardware address or client identifier. The DHCP server can provide the host’s IP address, domain name, gateway router and DNS server, information about the host’s boot image including the TFTP server to access for download and the name of the boot file, or boot information for NetBIOS Windows Internet Naming Service (WINS).

### Specifying A DHCP Client Identifier

Use the IP Service > DHCP > Client page to specify the DHCP client identifier for a VLAN interface.

### CLI REFERENCES

- "ip dhcp client class-id" on page 1039

### COMMAND USAGE

- The class identifier is used identify the vendor class and configuration of the switch to the DHCP server, which then uses this information to decide on how to service the client or the type of information to return.

- The general framework for this DHCP option is set out in RFC 2132 (Option 60). This information is used to convey configuration settings or other identification information about a client, but the specific string to use should be supplied by your service provider or network administrator.

### PARAMETERS

These parameters are displayed in the web interface:

- **VLAN** – ID of configured VLAN.

- **Vendor Class ID** – The following options are supported when the check box is marked to enable this feature:

  - **Default** – Depending the unit, the default string is EL326
  - **Text** – A text string. (Range: 1-32 characters)
  - **Hex** – A hexadecimal value.

### WEB INTERFACE

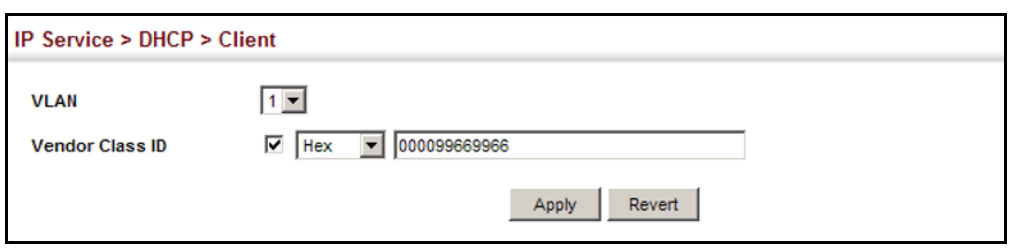
To configure a DHCP client identifier:

1. Click IP Service, DHCP, Client.

2. Mark the check box to enable this feature. Select the default setting, or the format for a vendor class identifier. If a non-default value is used, enter a text string or hexadecimal value.

3. Click Apply.

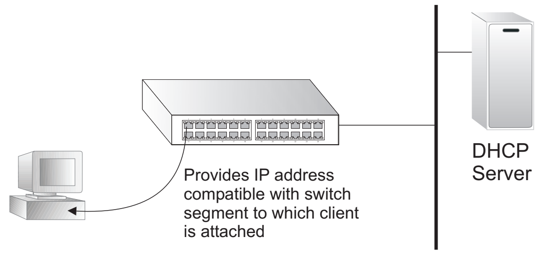
**Figure 9: Specifying A DHCP Client Identifier**




## Configuring DHCP Relay Service

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

**Figure 10: Layer 3 DHCP Relay Service**




### CLI REFERENCES

- "ip dhcp relay server" on page 1042
- "ip dhcp restart relay" on page 1042

### COMMAND USAGE

- You must specify the IP address for at least one DHCP server. Otherwise, the switch's DHCP relay agent will not forward client requests to a DHCP server.
- DHCP relay configuration will be disabled if an active DHCP server is detected on the same network segment.

### PARAMETERS

These parameters are displayed in the web interface:

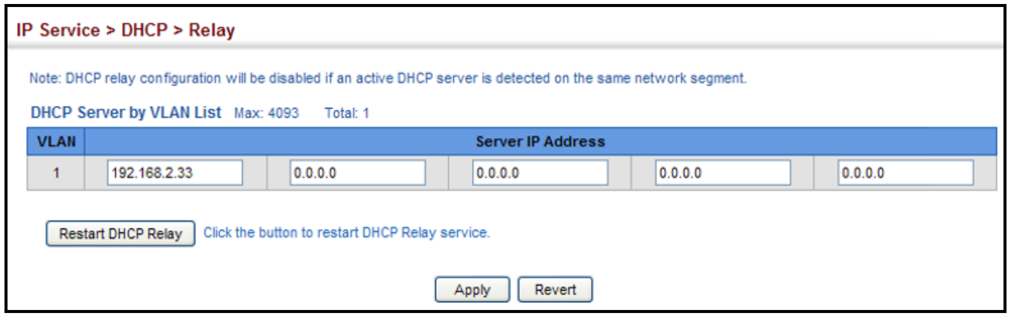
- **VLAN ID** – ID of configured VLAN.
- **Server IP Address** – Addresses of DHCP servers to be used by the switch's DHCP relay agent in order of preference.
- **Restart DHCP Relay** – Use this button to re-initialize DHCP relay service.

### WEB INTERFACE

To configure DHCP relay service:

1. Click IP Service, DHCP, Relay.
2. Enter up to five IP addresses for any VLAN.
3. Click Apply.

**Figure 11: Configuring DHCP Relay Service**

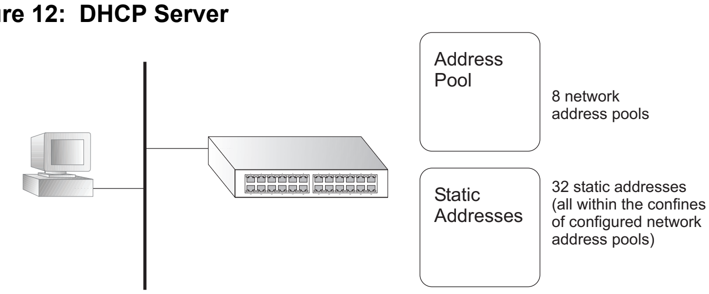



## Configuring the DHCP Server

This switch includes a Dynamic Host Configuration Protocol (DHCP) server that can assign temporary IP addresses to any attached host requesting service. It can also provide other network settings such as the domain name, default gateway, Domain Name Servers (DNS), Windows Internet Naming Service (WINS) name servers, or information on the bootup file for the host device to download.

Addresses can be assigned to clients from a common address pool configured for a specific IP interface on this switch, or fixed addresses can be assigned to hosts based on the client identifier code or MAC address.

**Figure 12: DHCP Server**




### Command Usage

- First configure any excluded addresses, including the address for this switch.
- Then configure address pools for the network interfaces. You can configure up to 8 network address pools. You can also manually bind an address to a specific client if required. However, any fixed addresses must fall within the range of an existing network address pool. You can configure up to 32 fixed host addresses (i.e., entering one address per pool).
- If the DHCP server is running, you must disable it and then reenable it to implement any configuration changes. This can be done on the IP Service > DHCP > Server (Configure Global) page.

### Enabling the Server

Use the IP Service > DHCP > Server (Configure Global) page to enable the DHCP Server.

### CLI References

- "service dhcp" on page 1045

### PARAMETERS

These parameters are displayed in the web interface:

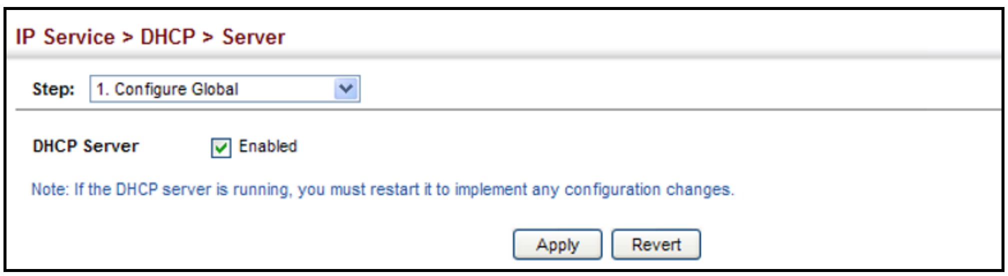
- **DHCP Server** – Enables or disables the DHCP server on this switch. (Default: Disabled)

### WEB INTERFACE

To enable the DHCP server:

1. Click IP Service, DHCP, Server.
2. Select Configure Global from the Step list.
3. Mark the Enabled box.
4. Click Apply.

**Figure 13: Enabling the DHCP Server**




## SETTING EXCLUDED ADDRESSES

Use the IP Service > DHCP > Server (Configure Excluded Addresses – Add) page to specify the IP addresses that should not be assigned to clients.

### CLI REFERENCES

- "ip dhcp excluded-address" on page 1044

### PARAMETERS

These parameters are displayed in the web interface:

- **Start IP Address** – Specifies a single IP address or the first address in a range that the DHCP server should not assign to DHCP clients.
- **End IP Address** – The last address in a range that the DHCP server should not assign to DHCP clients.

**NOTE:** Be sure you exclude the address for this switch and other key network devices.

### WEB INTERFACE

To configure IP addresses excluded for DHCP clients:

1. Click IP Service, DHCP, Server.

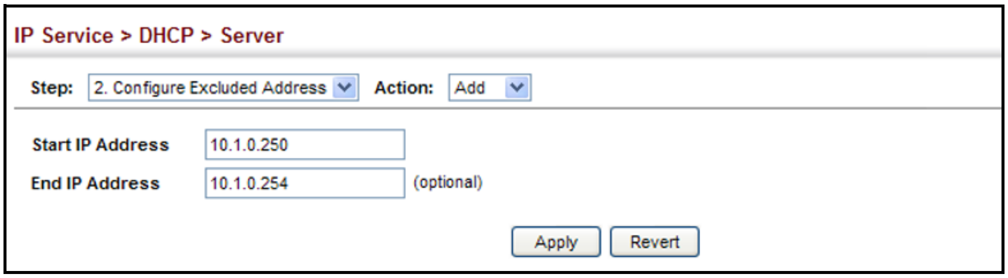
**2.** Select Configure Excluded Addresses from the Step list.

**3.** Select Add from the Action list.

**4.** Enter a single address or an address range.

**5.** Click Apply.

**Figure 14: Configuring Excluded Addresses on the DHCP Server**



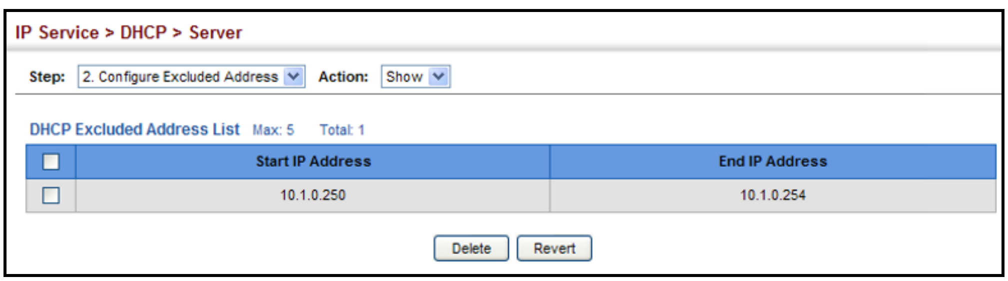

To show the IP addresses excluded for DHCP clients:

**1.** Click IP Service, DHCP, Server.

**2.** Select Configure Excluded Addresses from the Step list.

**3.** Select Show from the Action list.

**Figure 15: Showing Excluded Addresses on the DHCP Server**




### CONFIGURING ADDRESS POOLS

Use the IP Service > DHCP > Server (Configure Pool – Add) page configure IP address pools for each IP interface that will provide addresses to attached clients via the DHCP server.

#### CLI REFERENCES

■"DHCP Server" on page 1043

#### COMMAND USAGE

■First configure address pools for the network interfaces. Then you can manually bind an address to a specific client if required. However, note that any static host address must fall within the range of an existing network address pool. You can configure up to 8 network address pools, and up to 32 manually bound host address pools (i.e., one address per host pool). Just note that any address specified in a host address pool must fall within the range of a configured network address pool.

- When a client request is received, the switch first checks for a network address pool matching the gateway where the request originated (i.e., if the request was forwarded by a relay server). If there is no gateway in the client request (i.e., the request was not forwarded by a relay server), the switch searches for a network pool matching the interface through which the client request was received. It then searches for a manually configured host address that falls within the matching network pool. If no manually configured host address is found, it assigns an address from the matching network address pool. However, if no matching address pool is found the request is ignored.

- When searching for a manual binding, the switch compares the client identifier and then the hardware address for DHCP clients. Since BOOTP clients cannot transmit a client identifier, you must configure a hardware address for this host type. If no manual binding has been specified for a host entry with a hardware address or client identifier, the switch will assign an address from the first matching network pool.

- If the subnet mask is not specified for network or host address pools, the class A, B, or C natural mask is used (see "Specifying Network Interfaces" on page 491). The DHCP server assumes that all host addresses are available. You can exclude subsets of the address space by using the IP Service > DHCP > Server (Configure Excluded Addresses – Add) page.

### PARAMETERS

These parameters are displayed in the web interface:

*Creating a New Address Pool*

- **Pool Name** – A string or integer. (Range: 1-8 characters)

- **Type** – Sets the address pool type to Network or Host.

*Setting Parameters for a Network Pool*

- **IP** – The IP address of the DHCP address pool.

- **Subnet Mask** – The bit combination that identifies the network (or subnet) and the host portion of the DHCP address pool.

*Setting Parameters for a Static Host*

- **IP** – The IP address to assign to the host.

- **Subnet Mask** – Specifies the network mask of the client.

- **Client-Identifier** – A unique designation for the client device, either a text string (1-15 characters) or hexadecimal value. The information included in the identifier is based on RFC 2132 Option 60, and must be unique for all clients in the same administrative domain.

- **Hardware Address** – Specifies the MAC address and protocol used on the client. (Options: Ethernet, IEEE802, FDDI, None; Default: Ethernet)

*Setting Optional Parameters*

- **Default Router** – The IP address of the primary and alternate gateway router. The IP address of the router should be on the same subnet as the client.
- **DNS Server** – The IP address of the primary and alternate DNS server. DNS servers must be configured for a DHCP client to map host names to IP addresses.
- **Netbios Server** – IP address of the primary and alternate NetBIOS Windows Internet Naming Service (WINS) name server used for Microsoft DHCP clients.
- **Netbios Type** – NetBIOS node type for Microsoft DHCP clients. (Options: Broadcast, Hybrid, Mixed, Peer to Peer; Default: Hybrid)
- **Domain Name** – The domain name of the client. (Range: 1-128 characters)
- **Bootfile** – The default boot image for a DHCP client. This file should placed on the Trivial File Transfer Protocol (TFTP) server specified as the Next Server.
- **Next Server** – The IP address of the next server in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server.
- **Lease Time** – The duration that an IP address is assigned to a DHCP client. (Options: Finite, Infinite; Default: Infinite)

**WEB INTERFACE**

To configure DHCP address pools:

1. Click IP Service, DHCP, Server.
2. Select Configure Pool from the Step list.
3. Select Add from the Action list.
4. Set the pool Type to Network or Host.
5. Enter the IP address and subnet mask for a network pool or host. If configuring a static binding for a host, enter the client identifier or hardware address for the host device. Configure the optional parameters such as a gateway server and DNS server.
6. Click Apply.

**Figure 16: Configuring DHCP Server Address Pools** (Network)

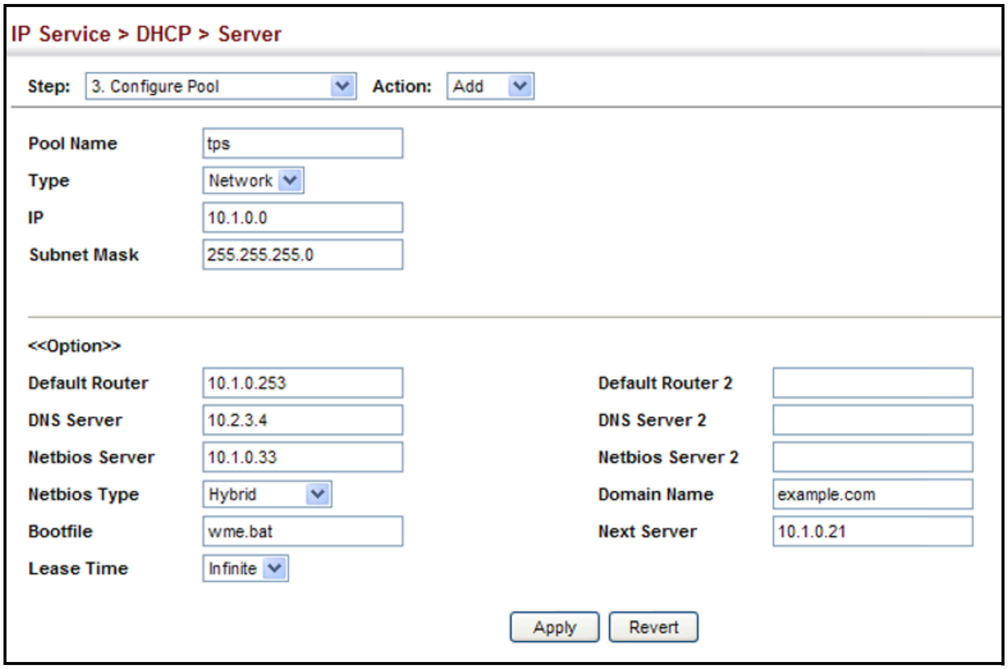
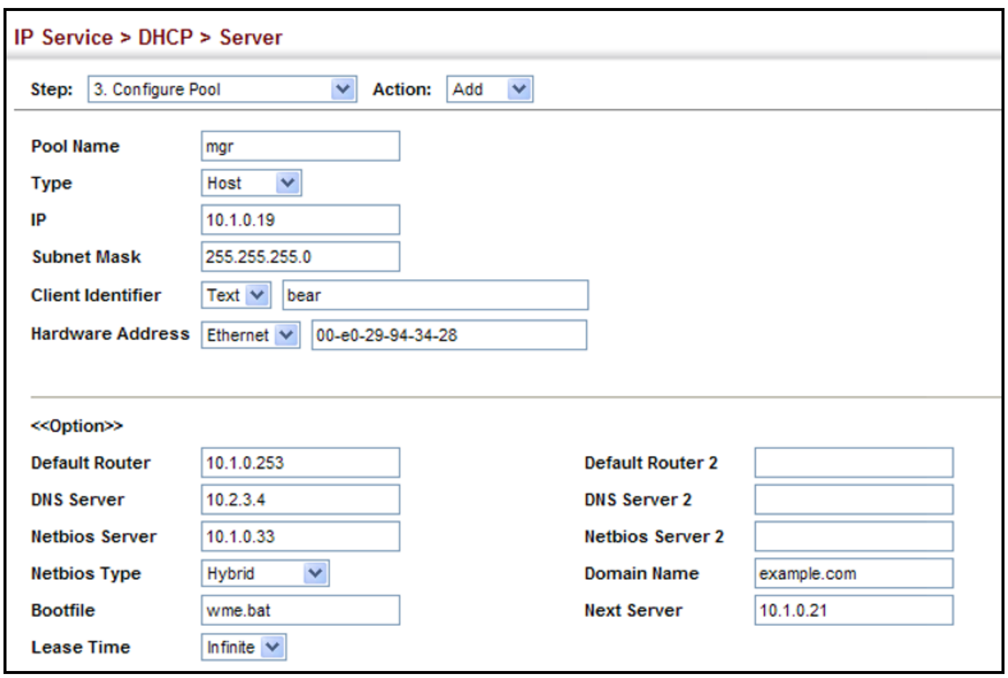


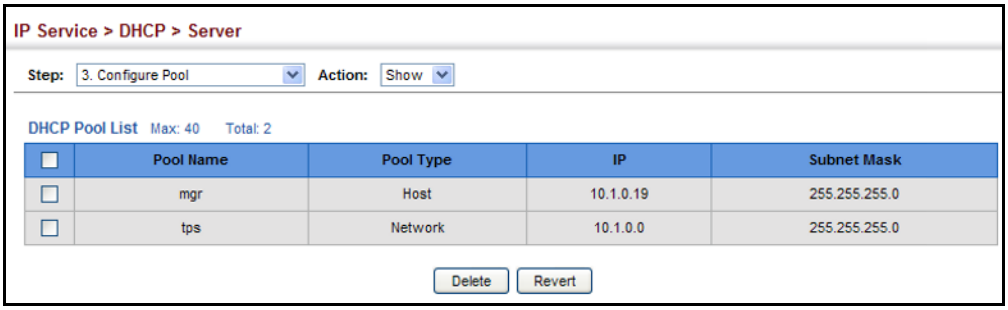

**Figure 17: Configuring DHCP Server Address Pools** (Host)




To show the configured DHCP address pools:

1. Click IP Service, DHCP, Server.
2. Select Configure Pool from the Step list.
3. Select Show from the Action list.

**Figure 18: Showing Configured DHCP Server Address Pools**


IP Service > DHCP > Server

Step: 3. Configure Pool Action: Show

DHCP Pool List Max: 40 Total: 2

| ☐ | Pool Name | Pool Type | IP | Subnet Mask |
|---|---|---|---|---|
| ☐ | mgr | Host | 10.1.0.19 | 255.255.255.0 |
| ☐ | tps | Network | 10.1.0.0 | 255.255.255.0 |

Delete Revert

## DISPLAYING ADDRESS BINDINGS

Use the IP Service > DHCP > Server (Show IP Binding) page display the host devices which have acquired an IP address from this switch's DHCP server.

### CLI REFERENCES

■ "show ip dhcp binding" on page 1054

### PARAMETERS

These parameters are displayed in the web interface:

■ **IP Address** – IP address assigned to host.

■ **MAC Address** – MAC address of host.

■ **Lease Time** – Duration that this IP address can be used by the host.

■ **Start Time** – Time this address was assigned by the switch.

### WEB INTERFACE

To show the addresses assigned to DHCP clients:

1. Click IP Service, DHCP, Server.

2. Select Show IP Binding from the Step list.

**Figure 19: Shows Addresses Assigned by the DHCP Server**


IP Service > DHCP > Server

Step: 4. Show IP Binding

IP Binding List Max: 512 Total: 1

| ☐ | IP Address | MAC Address | Lease Time | Start Time |
|---|---|---|---|---|
| ☐ | 192.168.2.61 | 00-60-6E-00-5F-A1 | Infinite | Dec 7 12:20:50 2009 |

Delete Revert

## FORWARDING UDP SERVICE REQUESTS

This section describes how this switch can forward UDP broadcast packets originating from host applications to another part of the network when an local application server is not available.

#### COMMAND USAGE

- Network hosts occasionally use UDP broadcasts to determine information such as address configuration, and domain name mapping. These broadcasts are confined to the local subnet, either as an all hosts broadcast (all ones broadcast - 255.255.255.255), or a directed subnet broadcast (such as 10.10.10.255). To reduce the number of application servers deployed in a multi-segment network, UDP helper can be used to forward broadcast packets for specified UDP application ports to remote servers located in another network segment.

- To configure UDP helper, enable it globally (see "Configuring General DNS Service Parameters" on page 465), specify the UDP destination ports for which broadcast traffic will be forwarded (see "Specifying UDP Destination Ports" on page 482), and specify the remote application servers or the subnet where the servers are located (see "Specifying The Target Server or Subnet" on page 483).

### Enabling the UDP Helper

Use the IP Service > UDP Helper > General page to enable the UDP helper globally on the switch.

#### CLI REFERENCES

- "ip helper" on page 1078

#### PARAMETERS

These parameters are displayed in the web interface:

- **UDP Helper Status** – Enables or disables the UDP helper. (Default: Disabled)

#### WEB INTERFACE

To enable the UDP help:

1. Click IP Service, UDP Helper, General.

2. Mark the Enabled check box.

3. Click Apply.

**Figure 20: Enabling the UDP Helper**

## Specifying UDP Destination Ports

Use the IP Service > UDP Helper > Forwarding page to specify the UDP destination ports for which broadcast traffic will be forwarded when the UDP helper is enabled.

#### CLI REFERENCES

■ "ip forward-protocol udp" on page 1077

#### COMMAND USAGE

■ Up to 100 UDP ports can be specified with this command for forwarding to one or more remote servers.

#### PARAMETERS

These parameters are displayed in the web interface:

■ **Destination UDP Port** – UDP application port for which UDP service requests are forwarded. (Range: 1-65535)

The following UDP ports are included in the forwarding list when the UDP helper is enabled, and a remote server address is configured:

BOOTP client port 67
BOOTP server port 68
Domain Name Service port 53
IEN-116 Name Service port 42
NetBIOS Datagram Server port 138
NetBIOS Name Server port 137
NTP port 37
TACACS service port 49
TFTP port 69

#### WEB INTERFACE

To specify UDP destination ports for forwarding:

1. Click IP Service, UDP Helper, Forwarding.

2. Select Add from the Action list.

3. Enter a destination UDP port number for which service requests are to be forwarded to a remote application server.

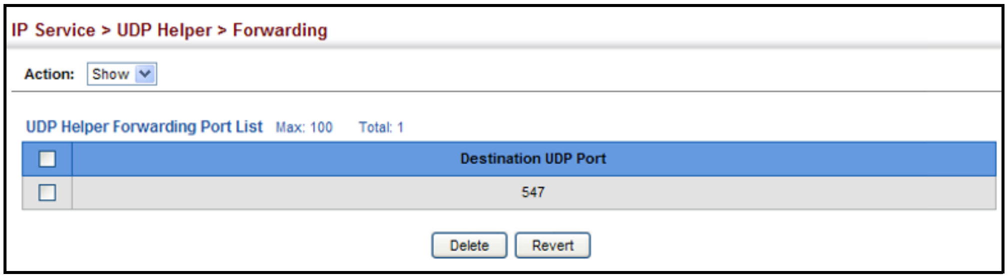
4. Click Apply.

**Figure 21: Specifying UDP Destination Ports**

To show the configured UDP destination ports:

1. Click IP Service, UDP Helper, Forwarding.
2. Select Show from the Action list.

**Figure 22: Showing the UDP Destination Ports**




## Specifying The Target Server or Subnet

Use the IP Service > UDP Helper > Address page to specify the application server or subnet (indicated by a directed broadcast address) to which designated UDP broadcast packets are forwarded.

### CLI REFERENCES

■ "ip helper-address" on page 1079

### COMMAND USAGE

■ Up to 20 helper addresses can be specified.

■ To forward UDP packets with the UDP helper, the clients must be connected to the selected interface, and the interface configured with an IP address.

■ The UDP packets to be forwarded must be specified in the IP Service > UDP Helper > Forwarding page, and the packets meet the following criteria:

- ◆ The MAC address of the received frame must be the all-ones broadcast address (ffff.ffff.ffff).
- ◆ The IP destination address must be one of the following:
  - ◆ all-ones broadcast (255.255.255.255)
  - ◆ subnet broadcast for the receiving interface
- ◆ The IP time-to-live (TTL) value must be at least 2.
- ◆ The IP protocol must be UDP (17).
- ◆ The UDP destination port must be TFTP, Domain Name System (DNS), Time, NetBIOS, BOOTP or DHCP packet, or a UDP port specified on the IP Service > UDP Helper > Forwarding page.

■ If a helper address is specified on this configuration page, but no UDP ports have been specified on the IP Service > UDP Helper > Forwarding page, broadcast traffic for several UDP protocol types will be forwarded by default as described on page 482.

### Parameters

These parameters are displayed in the web interface:

- **VLAN ID** – VLAN identifier (Range: 1-4093)
- **IP Address** – Host address or directed broadcast address to which UDP broadcast packets are forwarded. (Range: 1-65535)

### Web Interface

To specify the target server or subnet for forwarding UDP request packets:

1. Click IP Service, UDP Helper, Address.
2. Select Add from the Action list.
3. Enter the address of the remote server or subnet where UDP request packets are to be forwarded.
4. Click Apply.

**Figure 23: Specifying the Target Server or Subnet for UDP Requests**


To show the target server or subnet for UDP requests:

1. Click IP Service, UDP Helper, Address.
2. Select Show from the Action list.

**Figure 24: Showing the Target Server or Subnet for UDP Requests**

# 21 UNICAST ROUTING

This chapter describes how to configure the following unicast routing protocols:

RIP – Configures Routing Information Protocol.

OSPFv2 – Configures Open Shortest Path First (Version 2) for IPv4.

OSPFv3 – Configures Open Shortest Path First (Version 3) for IPv6.

## OVERVIEW

This switch can route unicast traffic to different subnetworks using the Routing Information Protocol (RIP) or Open Shortest Path First (OSPF) protocol. It supports RIP, RIP-2 and OSPFv2 and OSPFv3 dynamic routing. These protocols exchange routing information, calculate routing tables, and can respond to changes in the status or loading of the network.

*RIP and RIP-2 Dynamic Routing Protocols*

The RIP protocol is the most widely used routing protocol. RIP uses a distance-vector-based 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. Each router broadcasts its advertisement every 30 seconds, together with any updates to its routing table. This allows all routers on the network to learn consistent tables of next hop links which lead to relevant subnets.

**NOTE:** RIPng, which supports IPv6, will be supported in a future release.

*OSPFv2 and OSPFv3 Dynamic Routing Protocols*

OSPF overcomes all the problems of RIP. It 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. Moreover, when several equal-cost routes to a destination exist, traffic can be distributed equally among them.

OSPFv3, which supports routing for IPv6, uses the same basic mechanisms as OSPFv2, including the SPF algorithm, flooding of LSAs, and segregation into network areas. Most timers and metrics are also the same. However, note that OSPFv3 is not backward compatible with OSPFv2. Therefore, if you need to route both IPv4 and IPv6 packets, you will have to run both OSPFv2 and OSPFv3.

*Non-IP Protocol Routing*

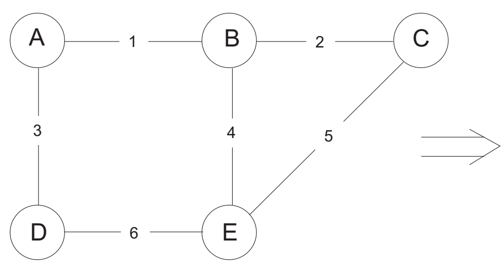
The switch supports IP routing only. Non-IP protocols such as IPX and Appletalk cannot be routed by this switch, and will be confined within their local VLAN group unless bridged by an external router.

To coexist with a network built on multilayer switches, the subnetworks for non-IP protocols must follow the same logical boundary as that of the IP subnetworks. A separate multi-protocol router can then be used to link the subnetworks by connecting to one port from each available VLAN on the network.

## CONFIGURING THE ROUTING INFORMATION PROTOCOL

The RIP protocol is the most widely used routing protocol. The RIP protocol uses a distance-vector-based 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. Each router broadcasts its advertisement every 30 seconds, together with any updates to its routing table. This allows all routers on the network to learn consistent tables of next hop links which lead to relevant subnets.

**Figure 1: Configuring RIP**




Cost = 1 for all links

| A | Link | Cost |
|---|---|---|
| A | 0 | 0 |
| B | 1 | 1 |
| C | 1 | 2 |
| D | 3 | 1 |
| E | 1 | 2 |

Routing table for node A

### COMMAND USAGE

- Just as Layer 2 switches use the Spanning Tree Algorithm to prevent loops, routers also use methods for preventing loops that would cause endless retransmission of data traffic. RIP utilizes the following three methods to prevent loops from occurring:
    - Split horizon – Never propagate routes back to an interface port from which they have been acquired.
    - Poison reverse – Propagate routes back to an interface port from which they have been acquired, but set the distance-vector metrics to infinity. (This provides faster convergence.)
    - Triggered updates – Whenever a route gets changed, broadcast an update message after waiting for a short random delay, but without waiting for the periodic cycle.
- RIP-2 is a compatible upgrade to RIP. RIP-2 adds useful capabilities for plain text authentication, multiple independent RIP domains, variable length subnet masks, and multicast transmissions for route advertising (RFC 1723).

- There are several serious problems with RIP that you should consider. First of all, RIP (version 1) has no knowledge of subnets, both RIP versions can take a long time to converge on a new route after the failure of a link or router during which time routing loops may occur, and its small hop count limitation of 15 restricts its use to smaller networks. Moreover, RIP (version 1) wastes valuable network bandwidth by propagating routing information via broadcasts; it also considers too few network variables to make the best routing decision.

## Configuring General Protocol Settings

Use the Routing Protocol > RIP > General (Configure) page to configure general settings and the basic timers.

RIP is used to specify how routers exchange routing information. When RIP is enabled on this router, it sends RIP messages to all devices in the network every 30 seconds (by default), and updates its own routing table when RIP messages are received from other routers. To communicate properly with other routers using RIP, you need to specify the RIP version used globally by the router, as well as the RIP send and receive versions used on specific interfaces (see "Configuring Network Interfaces for RIP" on page 498).

### CLI References

- "Routing Information Protocol (RIP)" on page 1120

### Command Usage

- RIP is used to specify how routers exchange routing information. When RIP is enabled on this router, it sends RIP messages to all devices in the network every 30 seconds (by default), and updates its own routing table when RIP messages are received from other routers. To communicate properly with other routers using RIP, you need to specify the RIP version used globally by the router, as well as the RIP send and receive versions used on specific interfaces (page 498).

### Parameters

These parameters are displayed in the web interface:

*Global Settings*

- **RIP Routing Process** – Enables RIP routing globally. RIP must also be enabled on each network interface which will participate in the routing process as described under "Specifying Network Interfaces" on page 491. (Default: Disabled)

- **Global RIP Version** – Specifies a RIP version used globally by the router. (Version 1, Version 2, By Interface; Default: By Interface)

  When a Global RIP Version is specified, any VLAN interface not previously set to a specific Receive or Send Version (page 498) is set to the following values:

  - RIP Version 1 configures previously unset interfaces to send RIPv1 compatible protocol messages and receive either RIPv1 or RIPv2 protocol messages.

  - RIP Version 2 configures previously unset interfaces to use RIPv2 for both sending and receiving protocol messages.

  RIP send/receive versions set on the RIP Interface settings screen (page 498) always take precedence over the settings for the Global RIP Version. However, when the Global RIP Version is set to “By Interface,” any VLAN interface not previously set to a specific receive or send version is set to the following default values:

- Receive: Accepts RIPv1 or RIPv2 packets.
- Send: Route information is broadcast to other routers with RIPv2.

- **RIP Default Metric** – Sets the default metric assigned to external routes imported from other protocols. (Range: 1-15; Default: 1)

  The default metric must be used to resolve the problem of redistributing external routes with incompatible metrics.

  It is advisable to use a low metric when redistributing routes from another protocol into RIP. Using a high metric limits the usefulness of external routes redistributed into RIP. For example, if a metric of 10 is defined for redistributed routes, these routes can only be advertised to routers up to 5 hops away, at which point the metric exceeds the maximum hop count of 15. By defining a low metric of 1, traffic can follow a imported route the maximum number of hops allowed within a RIP domain. However, note that using a low metric can increase the possibility of routing loops. For example, this can occur if there are multiple redistribution points and the router learns about the same external network with a better metric from a redistribution point other than that derived from the original source.

  The default metric does not override the metric value set in the Redistribute screen (see "Configuring Route Redistribution" on page 495). When a metric value has not been configured in the Redistribute screen, the default metric sets the metric value to be used for all imported external routes.

- **RIP Max Prefix** – Sets the maximum number of RIP routes which can be installed in the routing table. (Range: 1-7168; Default: 7168)

- **Default Information Originate** – Generates a default external route into the local RIP autonomous system. (Default: Disabled)

  A default route is set for every Layer 3 interface where RIP is enabled. The response packet to external queries marks each active RIP interface as a default router with the IP address 0.0.0.0.

- **Default Distance** – Defines an administrative distance for external routes learned from other routing protocols. External routes are routes for which the best path is learned from a neighbor external to the local RIP autonomous system. Routes with a distance of 255 are not installed in the routing table. (Range: 1-255; Default: 120)

  Administrative distance is used by the routers to select the preferred path when there are two or more different routes to the same destination from two different routing protocols. A smaller administrative distance indicates a more reliable protocol.

  Use the Routing Protocol > RIP > Distance page (see page 496) to configure the distance to a specific network address, or to configure an access list that filters networks according to the IP address of the router supplying the routing information.

- **Number of Route Changes** – The number of route changes made to the IP route database by RIP.

- **Number of Queries** – The number of responses sent to RIP queries from other systems.

*Basic Timer Settings*

**Note:** The timers must be set to the same values for all routers in the network.

- **Update** – Sets the rate at which updates are sent. This is the fundamental timer used to control all basic RIP processes. (Range: 5-2147483647 seconds; Default: 30 seconds)

  Setting the update timer to a short interval can cause the router to spend an excessive amount of time processing updates. On the other hand, setting it to an excessively long time will make the routing protocol less sensitive to changes in the network configuration.

- **Timeout** – Sets the time after which there have been no update messages that a route is declared dead. The route is marked inaccessible (i.e., the metric set to infinite) and advertised as unreachable. However, packets are still forwarded on this route. (Range: 90-360 seconds; Default: 180 seconds)

- **Garbage Collection** – After the *timeout* interval expires, the router waits for an interval specified by the *garbage-collection* timer before removing this entry from the routing table. This timer allows neighbors to become aware of an invalid route prior to purging. (Range: 60-240 seconds; Default: 120 seconds)

**Web Interface**

To configure general settings for RIP:

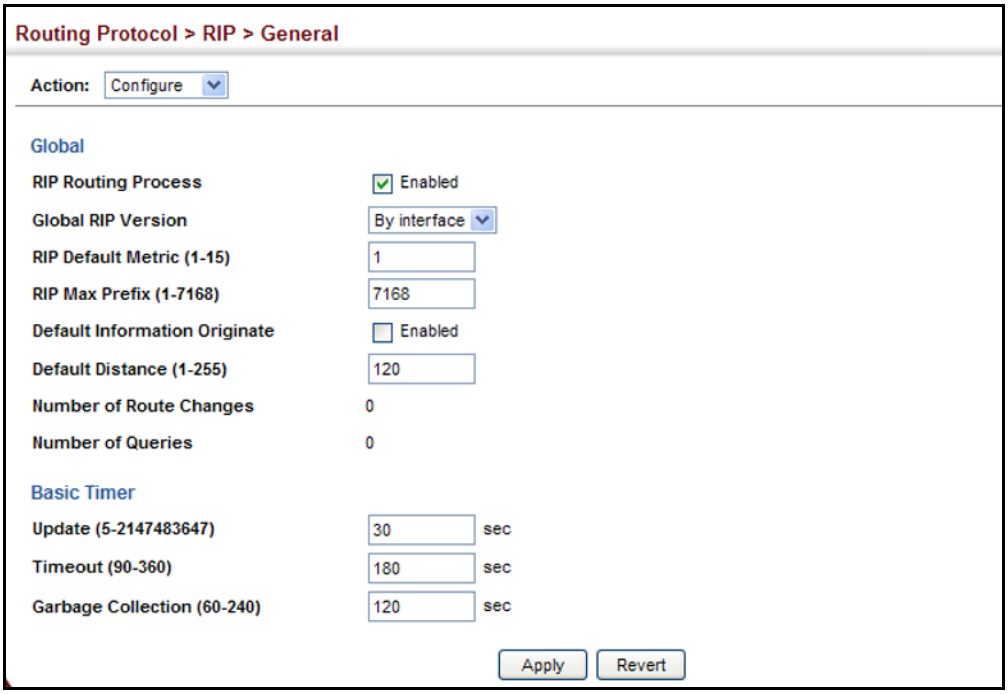
1. Click Routing Protocol, RIP, General.

2. Select Configure Global from the Action list.

3. Enable RIP, set the RIP version used on unset interfaces to RIPv1 or RIPv2, set the default metric assigned to external routes, set the maximum number of routes allowed by the system, and set the basic timers.

4. Click Apply.

**Figure 2: Configuring General Settings for RIP**




## CLEARING ENTRIES FROM THE ROUTING TABLE

Use the Routing Protocol > RIP > General (Clear Route) page to clear entries from the routing table based on route type or a specific network address.

### CLI REFERENCES

■ "clear ip rip route" on page 1135

### COMMAND USAGE

■ Clearing “All” types deletes all routes in the RIP table. To avoid deleting the entire RIP network, redistribute connected routes using the Routing Protocol > RIP > Redistribute screen (page 495) to make the RIP network a connected route. To delete the RIP routes learned from neighbors, but keep the RIP network intact, clear “RIP” types from the routing table.

### PARAMETERS

These parameters are displayed in the web interface:

■ **Clear Route By Type** – Clears entries from the RIP routing table based on the following types:

- **All** – Deletes all entries from the routing table.
- **Connected** – Deletes all currently connected entries.
- **OSPF** – Deletes all entries learned through OSPF.
- **RIP** – Deletes all entries learned through the RIP.
- **Static** – Deletes all static entries.

- **Clear Route By Network** – Clears a specific route based on its IP address and prefix length.
  - **Network IP Address** – Deletes all related entries for the specified network address.
  - **Prefix Length** – A decimal value indicating how many contiguous bits (from the left) of the address comprise the network portion of the address.

### WEB INTERFACE

To clear entries from the routing table RIP:

1. Click Routing Protocol, RIP, General.
2. Select Clear Route from the Action list.
3. When clearing routes by type, select the required type from the drop-down list. When clearing routes by network, enter a valid network address and prefix length.
4. Click Apply.

**Figure 3: Clearing Entries from the Routing Table**


## SPECIFYING NETWORK INTERFACES

Use the Routing Protocol > RIP > Network (Add) page to specify the network interfaces that will be included in the RIP routing process.

### CLI REFERENCES

- "network" on page 1125

### COMMAND USAGE

- RIP only sends and receives updates on specified interfaces. If a network is not specified, the interfaces in that network will not be advertised in any RIP updates.
- No networks are specified by default.

### PARAMETERS

These parameters are displayed in the web interface:

- **By Address** – Adds a network to the RIP routing process.
  - **Subnet Address** – IP address of a network directly connected to this router. (Default: No networks are specified)

- ◆ **Prefix Length** – A decimal value indicating how many contiguous bits (from the left) of the address comprise the network portion of the address. This mask identifies the network address bits used for the associated routing entries.

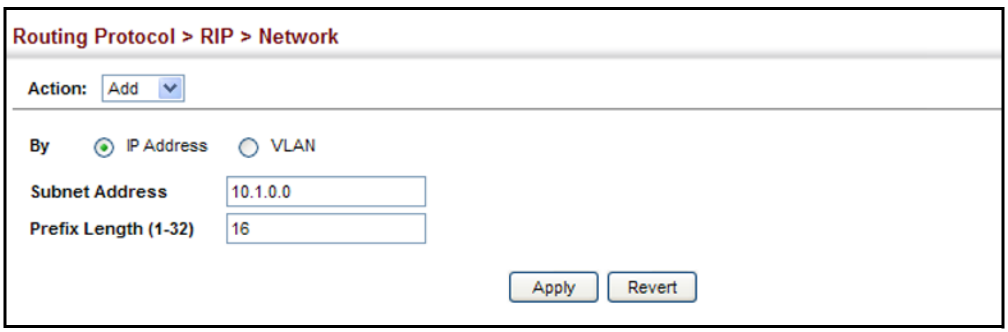
■**By VLAN** – Adds a Layer 3 VLAN to the RIP routing process. The VLAN must be configured with an IP address. (Range: 1-4093)

### WEB INTERFACE

To add a network interface to RIP:

1. Click Routing Protocol, RIP, Network.
2. Select Add from the Action list.
3. Add an interface that will participate in RIP.
4. Click Apply.

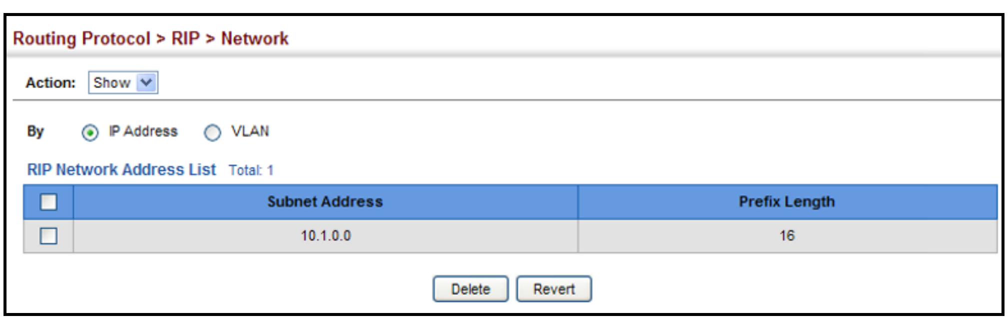
**Figure 4: Adding Network Interfaces to RIP**




To show the network interfaces using RIP:

1. Click Routing Protocol, RIP, Network.
2. Select Show from the Action list.
3. Click IP Address or VLAN.

**Figure 5: Showing Network Interfaces Using RIP**



## SPECIFYING PASSIVE INTERFACES

Use the Routing Protocol > RIP > Passive Interface (Add) page to stop RIP from sending routing updates on the specified interface.

### CLI REFERENCES

- "passive-interface" on page 1126

### COMMAND USAGE

- Network interfaces can be configured to stop RIP broadcast and multicast messages from being sent. If the sending of routing updates is blocked on an interface, the attached subnet will still continue to be advertised to other interfaces, and updates from other routers on the specified interface will continue to be received and processed.

- This feature can be used in conjunction with the static neighbor feature (described in the next section) to control the routing updates sent to specific neighbors.

### PARAMETERS

These parameters are displayed in the web interface:

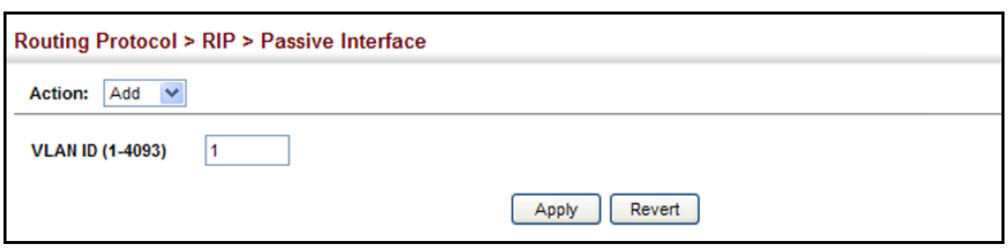
- **VLAN** – VLAN interface on which to stop sending RIP updates. (Range: 1-4093)

### WEB INTERFACE

To specify a passive RIP interface:

1. Click Routing Protocol, RIP, Passive Interface.
2. Select Add from the Action list.
3. Add the interface on which to stop sending RIP updates.
4. Click Apply.

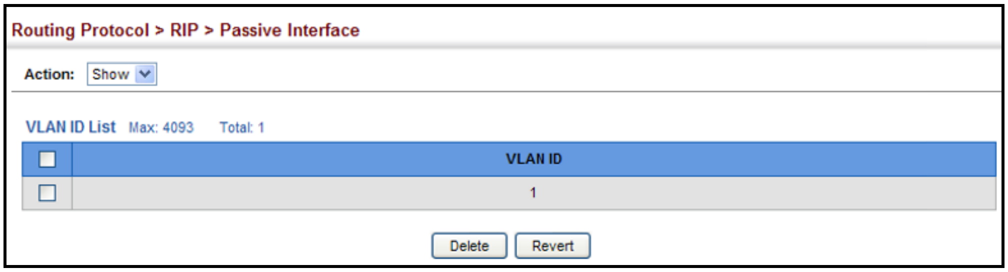
**Figure 6: Specifying a Passive RIP Interface**




To show the passive RIP interfaces:

1. Click Routing Protocol, RIP, Passive Interface.
2. Select Show from the Action list.

**Figure 7: Showing Passive RIP Interfaces**




## SPECIFYING STATIC NEIGHBORS

Use the Routing Protocol > RIP > Passive Interface (Add) page to configure this router to directly exchange routing information with a static neighbor (specifically for point-to-point links), rather than relying on broadcast or multicast messages generated by the RIP protocol. This feature can be used in conjunction with the passive interface feature (described in the preceding section) to control the routing updates sent to specific neighbors.

### CLI REFERENCES

- "neighbor" on page 1125

### PARAMETERS

These parameters are displayed in the web interface:

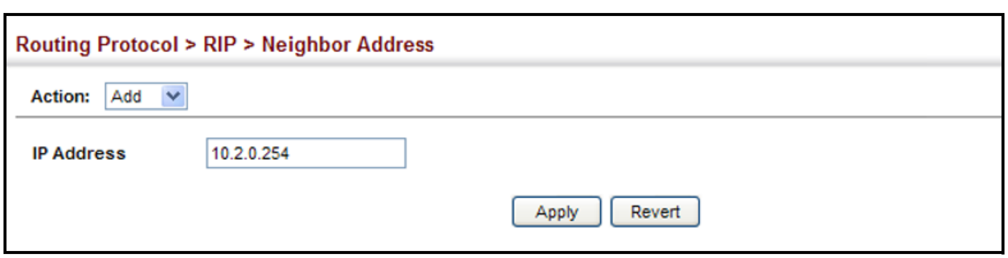
- **IP Address** – IP address of a static neighboring router with which to exchange routing information.

### WEB INTERFACE

To specify a static RIP neighbor:

1. Click Routing Protocol, RIP, Neighbor Address.
2. Select Add from the Action list.
3. Add the address of any static neighbors which may not readily to discovered through RIP.
4. Click Apply.

**Figure 8: Specifying a Static RIP Neighbor**

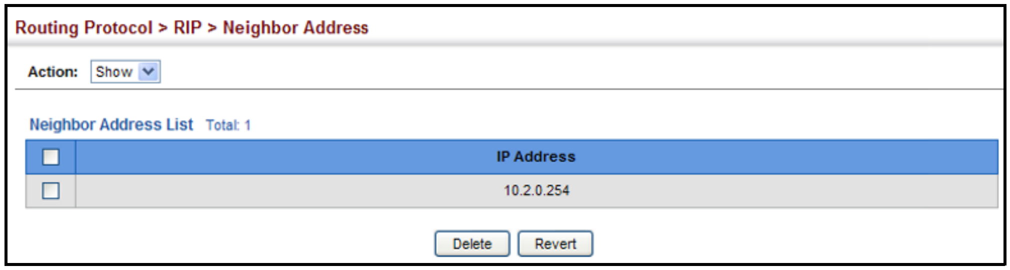


To show static RIP neighbors:

1. Click Routing Protocol, RIP, Neighbor Address.

2. Select Show from the Action list.

**Figure 9: Showing Static RIP Neighbors**




## CONFIGURING ROUTE REDISTRIBUTION

Use the Routing Protocol > RIP > Redistribute (Add) page to import external routing information from other routing domains (that is, directly connected routes, protocols, or static routes) into this autonomous system.

### CLI REFERENCES

■ "redistribute" on page 1127

### PARAMETERS

These parameters are displayed in the web interface:

■ **Protocol** – The type of routes that can be imported include:

- ◆ **Connected** – Imports routes that are established automatically just by enabling IP on an interface.
- ◆ **Static** – Static routes will be imported into this routing domain.
- ◆ **OSPF** – External routes will be imported from the Open Shortest Path First protocol into this routing domain.

■ **Metric** – Metric assigned to all external routes for the specified protocol. (Range: 0-16; Default: the default metric as described under "Configuring General Protocol Settings" on page 487.)

A route metric must be used to resolve the problem of redistributing external routes with incompatible metrics.

When a metric value has not been configured on this page, the default-metric determines the metric value to be used for all imported external routes.

It is advisable to use a low metric when redistributing routes from another protocol into RIP. Using a high metric limits the usefulness of external routes redistributed into RIP. For example, if a metric of 10 is defined for redistributed routes, these routes can only be advertised to routers up to 5 hops away, at which point the metric exceeds the maximum hop count of 15. By defining a low metric of 1, traffic can follow an imported route the maximum number of hops allowed within a RIP domain. However, using a low metric can increase the possibility of routing loops

For example, this can occur if there are multiple redistribution points and the router learns about the same external network with a better metric from a redistribution point other than that derived from the original source.

### WEB INTERFACE

To import external routing information from other routing domains:

1. Click Routing Protocol, RIP, Redistribute.
2. Select Add from the Action list.
3. Specify the protocol types (directly connected, OSPF or static) from which to import external routes, and the metric to assign to these routes.
4. Click Apply.

**Figure 10: Redistributing External Routes into RIP**


To show external routes imported into RIP:

1. Click Routing Protocol, RIP, Redistribute.
2. Select Show from the Action list.

**Figure 11: Showing External Routes Redistributed into RIP**


### SPECIFYING AN ADMINISTRATIVE DISTANCE

Use the Routing Protocol > RIP > Distance (Add) page to define an administrative distance for external routes learned from other routing protocols.

### CLI REFERENCES

- "distance" on page 1123

### COMMAND USAGE

- Administrative distance is used by the routers to select the preferred path when there are two or more different routes to the same destination from two different routing protocols. A smaller administrative distance indicates a more reliable protocol.
- An access list can be used to filter networks according to the IP address of the router supplying the routing information. For example, to filter out unreliable routing information from routers not under your administrative control.
- The administrative distance is applied to all routes learned for the specified network.

### PARAMETERS

These parameters are displayed in the web interface:

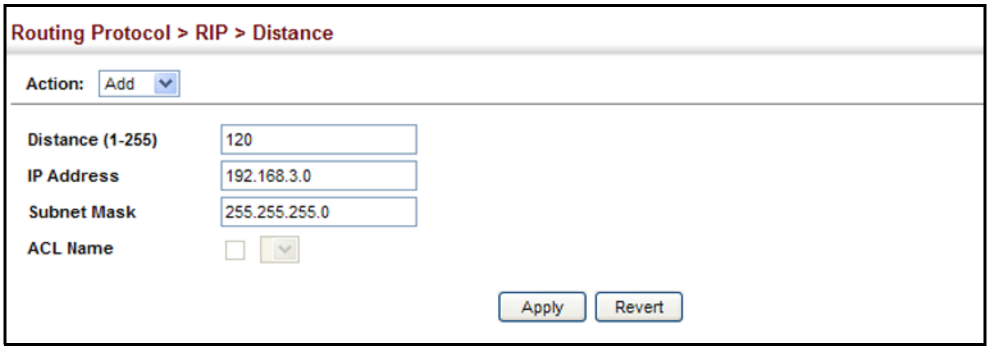
- **Distance** – Administrative distance for external routes. External routes are routes for which the best path is learned from a neighbor external to the local RIP autonomous system. Routes with a distance of 255 are not installed in the routing table. (Range: 1-255)
- **IP Address** – IP address of a route entry.
- **Subnet Mask** – This mask identifies the host address bits used for associated routing entries.
- **ACL Name** – Name of the access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs. (Range: 1-16 characters)

### WEB INTERFACE

To define an administrative distance for external routes learned from other routing protocols:

1. Click Routing Protocol, RIP, Distance.
2. Select Add from the Action list.
3. Enter the distance, the external route, and optionally enter the name of an ACL to filter networks according to the IP address of the router supplying the routing information.
4. Click Apply.

**Figure 12: Setting the Distance Assigned to External Routes**

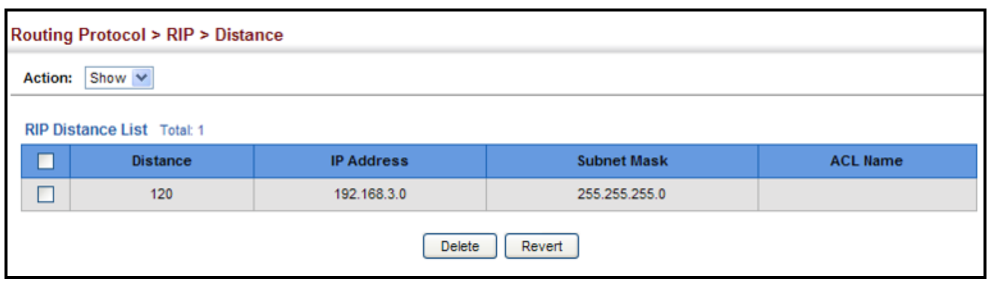



To show the distance assigned to external routes learned from other routing protocols:

1. Click Routing Protocol, RIP, Distance.

2. Select Show from the Action list.

**Figure 13: Showing the Distance Assigned to External Routes**




## CONFIGURING NETWORK INTERFACES FOR RIP

Use the Routing Protocol > RIP > Distance (Add) page to configure the send/receive version, authentication settings, and the loopback prevention method for each interface that participates in the RIP routing process.

### CLI REFERENCES

- "ip rip receive version" on page 1131
- "ip rip send version" on page 1133
- "ip rip authentication mode" on page 1130
- "ip rip authentication string" on page 1130
- "ip rip split-horizon" on page 1134

### COMMAND USAGE

*Specifying Receive and Send Protocol Types*

- Specify the protocol message type accepted (that is, RIP version) and the message type sent (that is, RIP version or compatibility mode) for each RIP interface.

- Setting the RIP Receive Version or Send Version for an interface overrides the global setting specified in the RIP General Settings screen (see "Configuring General Protocol Settings" on page 487).

- The Send Version can be specified based on these options:

- ◆ Use “RIPv1” or “RIPv2” if all routers in the local network are based on RIPv1 or RIPv2, respectively.
- ◆ Use “RIPv1 Compatible” to propagate route information by broadcasting to other routers on the network using the RIPv2 advertisement list, instead of multicasting as normally required by RIPv2. (Using this mode allows older RIPv2 routers which only receive RIP broadcast messages to receive all of the information provided by RIPv2, including subnet mask, next hop and authentication information. (This is the default setting.)
- ◆ Use “Do Not Send” to passively monitor route information advertised by other routers attached to the network.

■The Receive Version can be specified based on these options:

- ◆ Use “RIPv1” or “RIPv2” if all routers in the local network are based on RIPv1 or RIPv2, respectively.
- ◆ Use “RIPv1 and RIPv2” if some routers in the local network are using RIPv2, but there are still some older routers using RIPv1. (This is the default setting.)
- ◆ Use “Do Not Receive” if dynamic entries are not required to be added to the routing table for an interface. (For example, when only static routes are to be allowed for a specific interface.)

*Protocol Message Authentication*

RIPv1 is not a secure protocol. Any device sending protocol messages from UDP port 520 will be considered a router by its neighbors. Malicious or unwanted protocol messages can be easily propagated throughout the network if no authentication is required.

RIPv2 supports authentication using a simple password or MD5 key encryption. When a router is configured to exchange authentication messages, it will insert the password into all transmitted protocol packets, and check all received packets to ensure that they contain the authorized password. If any incoming protocol messages do not contain the correct password, they are simply dropped.

For authentication to function properly, both the sending and receiving interface must be configured with the same password or authentication key.

*Loopback Prevention*

Just as Layer 2 switches use the Spanning Tree Algorithm to prevent loops, routers also use methods for preventing loops that would cause endless retransmission of data traffic. When protocol packets are caught in a loop, links will be congested, and protocol packets may be lost. However, the network will slowly converge to the new state. RIP supports several methods which can provide faster convergence when the network topology changes and prevent most loops from occurring.

**PARAMETERS**

These parameters are displayed in the web interface:

■**VLAN ID** – Layer 3 VLAN interface. This interface must be configured with an IP address and have an active link. (Range: 1-4093)

- **Send Version** – The RIP version to send on an interface.
  - **RIPv1**: Sends only RIPv1 packets.
  - **RIPv2**: Sends only RIPv2 packets.
  - **RIPv1 Compatible**: Route information is broadcast to other routers with RIPv2.
  - **Do Not Send**: Does not transmit RIP updates. Passively monitors route information advertised by other routers attached to the network.

  The default depends on the setting for the Global RIP Version. (See "Configuring General Protocol Settings" on page 487.)

- **Receive Version** – The RIP version to receive on an interface.
  - **RIPv1**: Accepts only RIPv1 packets.
  - **RIPv2**: Accepts only RIPv2 packets.
  - **RIPv1 or RIPv2**: Accepts RIPv1 or RIPv2 packets.
  - **Do Not Receive**: Does not accept incoming RIP packets. This option does not add any dynamic entries to the routing table for an interface.

  The default depends on the setting for the Global RIP Version. (See "Configuring General Protocol Settings" on page 487.)

- **Authentication Type** – Specifies the type of authentication required for exchanging RIPv2 protocol messages. (Default: No Authentication)
  - **No Authentication**: No authentication is required.
  - **Simple Password**: Requires the interface to exchange routing information with other routers based on an authorized password. (Note that authentication only applies to RIPv2.)
  - **MD5**: Message Digest 5 (MD5) authentication.

    MD5 is a one-way hash algorithm is that takes the authentication key and produces a 128 bit message digest or “fingerprint.” This makes it computationally infeasible to produce two messages having the same message digest, or to produce any message having a given pre-specified target message digest.

- **Authentication Key** – Specifies the key to use for authenticating RIPv2 packets. For authentication to function properly, both the sending and receiving interface must use the same password. (Range: 1-16 characters, case sensitive)

- **Instability Prevention** – Specifies the method used to reduce the convergence time when the network topology changes, and to prevent RIP protocol messages from looping back to the source router.

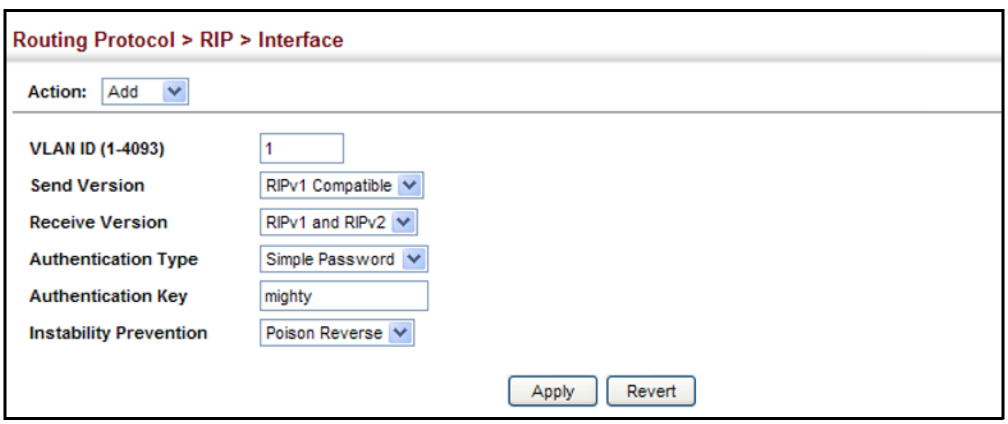
- **Split Horizon** – This method never propagate routes back to an interface from which they have been acquired.
- **Poison Reverse** – This method propagates routes back to an interface from which they have been acquired, but sets the distance-vector metrics to infinity. This provides faster convergence. (This is the default setting.)
- **None** – No loopback prevention method is employed. If a loop occurs without using any prevention method, the hop count for a route may be gradually incremented to infinity (that is, 16) before the route is deemed unreachable.

### WEB INTERFACE

To network interface settings for RIP:

1. Click Routing Protocol, RIP, Interface.
2. Select Add from the Action list.
3. Select a Layer 3 VLAN interface to participate in RIP. Select the RIP protocol message types that will be received and sent. Select the RIP authentication method and password. And then set the loopback prevention method.
4. Click Apply.

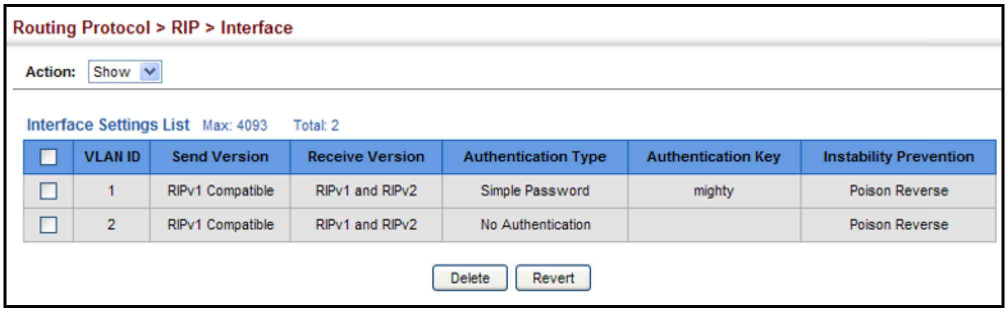
**Figure 14: Configuring a Network Interface for RIP**




To show the network interface settings configured for RIP:

1. Click Routing Protocol, RIP, Interface.
2. Select Show from the Action list.

**Figure 15: Showing RIP Network Interface Settings**




## DISPLAYING RIP INTERFACE SETTINGS

Use the Routing Protocol > RIP > Statistics (Show Interface Information) page to display information about RIP interface configuration settings.

### CLI REFERENCES

- "show ip rip" on page 1136

### PARAMETERS

These parameters are displayed in the web interface:

- **Interface** – Source IP address of RIP router interface.
- **Auth Type** – The type of authentication used for exchanging RIPv2 protocol messages.
- **Send Version** – The RIP version to sent on this interface.
- **Receive Version** – The RIP version accepted on this interface.
- **Rcv Bad Packets** – Number of bad RIP packets received.
- **Rcv Bad Routes** – Number of bad routes received.
- **Send Updates** – Number of route changes.

### WEB INTERFACE

To display RIP interface configuration settings:

1. Click Routing Protocol, RIP, Statistics.
2. Select Show Interface Information from the Action list.

**Figure 16: Showing RIP Interface Settings**

Routing Protocol > RIP > Statistics

Action: Show Interface Information

Interface Information Max: 4093 Total: 3

| Interface | Auth Type | Send Version | Receive Version | Rcv Bad Packets | Rcv Bad Routes | Send Updates |
|---|---|---|---|---|---|---|
| 1.2.3.4 | No Authentication | Do Not Send | RIPv1 and RIPv2 | 10 | 2 | 124 |
| 10.1.0.1 | Simple Password | RIPv1 | Do Not Receive | 3 | 4 | 23 |
| 140.113.1.3 | MD5 | RIPv1 Compatible | RIPv2 | 5 | 5 | 65 |

## DISPLAYING PEER ROUTER INFORMATION

Use the Routing Protocol > RIP > Statistics (Show Peer Information) page to display information on neighboring RIP routers.

### CLI REFERENCES

■ "show ip protocols rip" on page 1136

### PARAMETERS

These parameters are displayed in the web interface:

■ **Peer Address** – IP address of a neighboring RIP router.

■ **Update Time** – Last time a route update was received from this peer.

■ **Version** – Shows whether RIPv1 or RIPv2 packets were received from this peer.

■ **Rcv Bad Packets** – Number of bad RIP packets received from this peer.

■ **Rcv Bad Routes** – Number of bad routes received from this peer.

### WEB INTERFACE

To display information on neighboring RIP routers:

1. Click Routing Protocol, RIP, Statistics.

2. Select Show Peer Information from the Action list.

**Figure 17: Showing RIP Peer Information**

Routing Protocol > RIP > Statistics

Action: Show Peer Information

Peer Information Total: 2

| Peer Address | Update Time | Version | Rcv Bad Packets | Rcv Bad Routes |
|---|---|---|---|---|
| 10.2.3.0 | 10 | RIPv1 | 2 | 123 |
| 10.1.0.0 | 113 | RIPv2 | 4 | 23 |

## RESETTING RIP STATISTICS

Use the Routing Protocol > RIP > Statistics (Reset Statistics) page to reset all statistics for RIP protocol messages.

### CLI REFERENCES

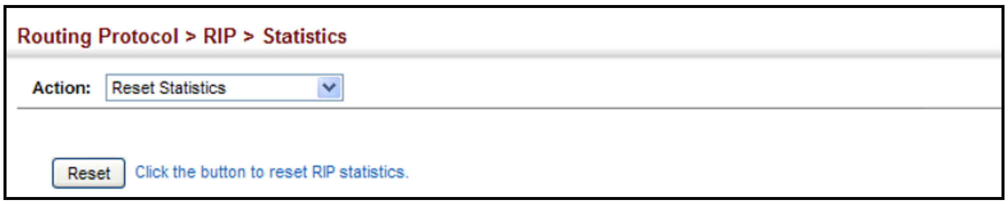
■ no comparable command

### WEB INTERFACE

To reset RIP statistics:

1. Click Routing Protocol, RIP, Statistics.
2. Select Reset Statistics from the Action list.
3. Click Reset.

**Figure 18: Resetting RIP Statistics**

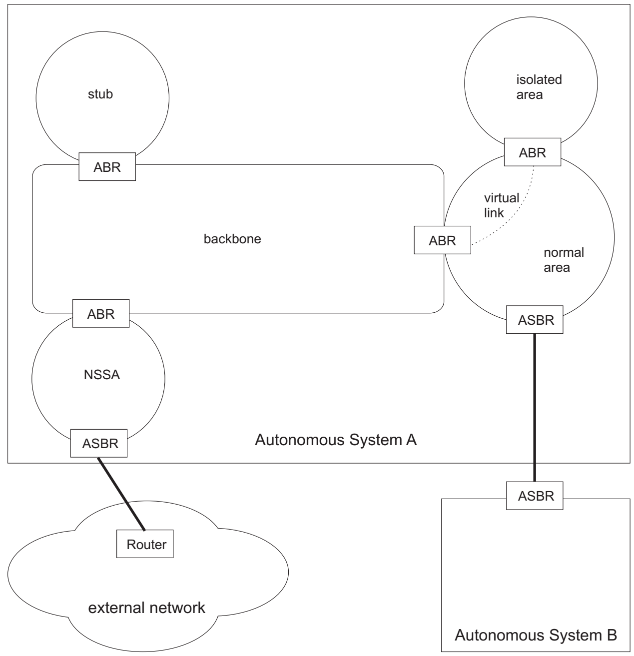



## CONFIGURING THE OPEN SHORTEST PATH FIRST PROTOCOL (VERSION 2)

Open Shortest Path First (OSPF) is more suited for large area networks which experience frequent changes in the links. It also handles subnets much better than RIP. OSPF protocol actively tests the status of each link to its neighbors to generate a shortest path tree, and builds a routing table based on this information. OSPF then utilizes IP multicast to propagate routing information. A separate routing area scheme is also used to further reduce the amount of routing traffic.

**NOTE:** The OSPF protocol implemented in this device is based on RFC 2328 (Version 2). It also supports RFC 1583 (early Version 2) compatibility mode to ensure that the same method is used to calculate summary route costs throughout the network when older OSPF routers exist; as well as the not-so-stubby area option (RFC 3101).

**Figure 19: Configuring OSPF**




## COMMAND USAGE

- OSPF looks at more than just the simple hop count. When adding the shortest path to any node into the tree, the optimal path is chosen on the basis of delay, throughput and connectivity. OSPF utilizes IP multicast to reduce the amount of routing traffic required when sending or receiving routing path updates. The separate routing area scheme used by OSPF further reduces the amount of routing traffic, and thus inherently provides another level of routing protection. In addition, all routing protocol exchanges can be authenticated. Finally, the OSPF algorithms have been tailored for efficient operation in TCP/IP Internets.

- OSPFv2 is a compatible upgrade to OSPF. It involves enhancements to protocol message authentication, and the addition of a point-to-multipoint interface which allows OSPF to run over non-broadcast networks, as well as support for overlapping area ranges.

- When using OSPF, you must organize your network (i.e., autonomous system) into normal, stub, or not-so-stubby areas; configure the ranges of subnet addresses that can be aggregated by link state advertisements; and configure virtual links for areas that do not have direct physical access to the OSFP backbone.

  - To implement OSPF for a large network, you must first organize the network into logical areas to limit the number of OSPF routers that actively exchange Link State Advertisements (LSAs). You can then define an OSPF interface by assigning an IP interface configured on this router to one of these areas. This OSPF interface will send and receive OSPF traffic to neighboring OSPF routers.

  - You can further optimize the exchange of OSPF traffic by specifying an area range that covers a large number of subnetwork addresses. This is an important technique for limiting the amount of traffic exchanged between Area Border Routers (ABRs).

- And finally, you must specify a virtual link to any OSPF area that is not physically attached to the OSPF backbone. Virtual links can also be used to provide a redundant link between contiguous areas to prevent areas from being partitioned, or to merge backbone areas. (Note that virtual links are not supported for stubs or NSSAs.)

## DEFINING NETWORK AREAS BASED ON ADDRESSES

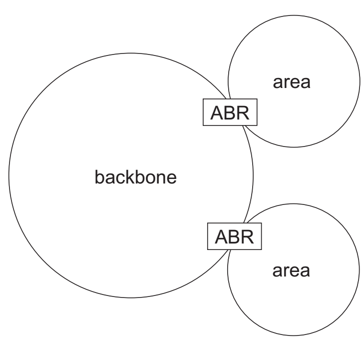
OSPF protocol broadcast messages (i.e., Link State Advertisements or LSAs) are restricted by area to limit their impact on network performance. A large network should be split up into separate OSPF areas to increase network stability, and to reduce protocol traffic by summarizing routing information into more compact messages. Each router in an area shares the same view of the network topology, including area links, route summaries for directly connected areas, and external links to other areas.

Use the Routing Protocol > OSPF > Network Area (Add) page to define an OSPF area and the interfaces that operate within this area. An autonomous system must be configured with a backbone area, designated by the area identifier 0.0.0.0. By default, all other areas are created as normal transit areas.

Routers in a normal area may import or export routing information about individual nodes. To reduce the amount of routing traffic flooded onto the network, an area can be configured to export a single summarized route that covers a broad range of network addresses within the area (page 520). To further reduce the amount of routes passed between areas, an area can be configured as a stub (page 513, page 517) or a not-so-stubby area (page 513, page 514).

*Normal Area* – A large OSPF domain should be broken up into several areas to increase network stability and reduce the amount of routing traffic required through the use of route summaries that aggregate a range of addresses into a single route. The backbone or any normal area can pass traffic between other areas, and are therefore known as transit areas. Each router in an area has identical routing tables. These tables may include area links, summarized links, or external links that depict the topology of the autonomous system.

**Figure 20: OSPF Areas**




### CLI REFERENCES

■"router ospf" on page 1139
■"network area" on page 1153

**COMMAND USAGE**

- Specify an Area ID and the corresponding network address range for each OSPF broadcast area. Each area identifies a logical group of OSPF routers that actively exchange Link State Advertisements (LSAs) to ensure that they share an identical view of the network topology.

- Each area must be connected to a backbone area. This area passes routing information between other areas in the autonomous system. All routers must be connected to the backbone, either directly, or through a virtual link if a direct physical connection is not possible.

- All areas are created as normal transit areas using the Network Area (Add) page. A normal area (or transit area) can send and receive external LSAs. If necessary, an area can be configured as a not-so-stubby area (NSSA) that can import external route information into its area, or as a stubby area that cannot send or receive external LSAs.

- An area must be assigned a range of subnetwork addresses. This area and the corresponding address range forms a routing interface, and can be configured to aggregate LSAs from all of its subnetwork addresses and exchange this information with other routers in the network as described under "Configuring Area Ranges (Route Summarization for ABRs)" on page 520.

- If an address range overlaps other network areas, the router will use the network area with the address range that most closely matches the interface address. Also, note that if a more specific address range is removed from an area, the interface belonging to that range may still remain active if a less specific address range covering that area has been specified.

**PARAMETERS**

These parameters are displayed in the web interface:

- **Process ID** – Protocol identifier used to distinguish between multiple routing instances. (Range: 1-65535)

- **IP Address** – Address of the interfaces to add to the area.

- **Netmask** – Network mask of the address range to add to the area.

- **Area ID** – Area to which the specified address or range is assigned. An OSPF area identifies a group of routers that share common routing information. The area ID can be in the form of an IPv4 address, or as a four octet unsigned integer ranging from 0-4294967295.

  Set the area ID to the same value for all routers on a network segment using the network mask to add one or more interfaces to an area.

**WEB INTERFACE**

To define an OSPF area and the interfaces that operate within this area:

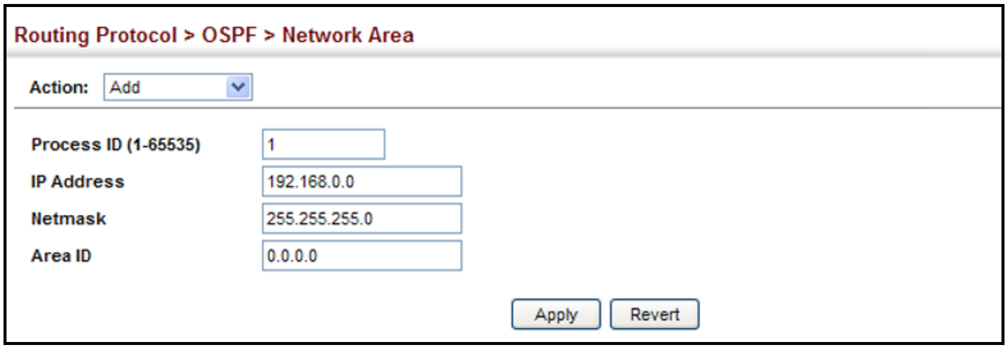
1. Click Routing Protocol, OSPF, Network Area.

2. Select Add from the Action list.

3. Configure a backbone area that is contiguous with all the other areas in the network, and configure an area for all of the other OSPF interfaces.

4. Click Apply

**Figure 21: Defining OSPF Network Areas Based on Addresses**

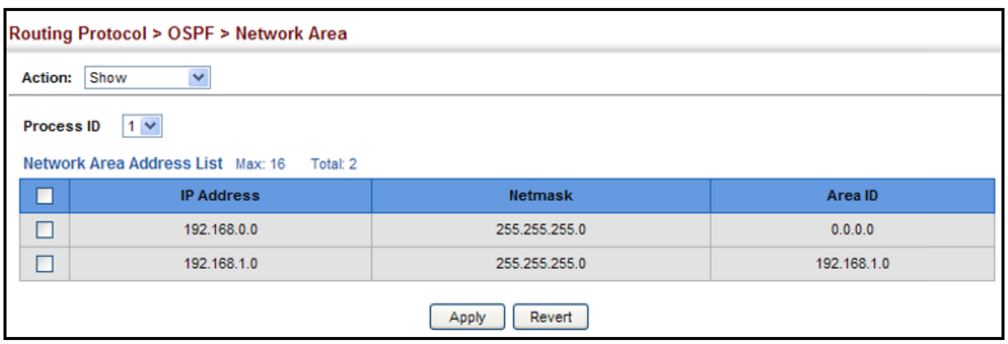



To to show the OSPF areas and the assigned interfaces:

1. Click Routing Protocol, OSPF, Network Area.

2. Select Show from the Action list.

**Figure 22: Showing OSPF Network Areas**

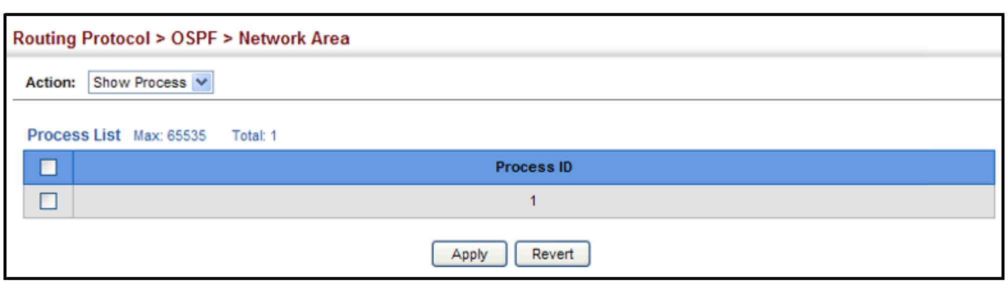



To to show the OSPF process identifiers:

1. Click Routing Protocol, OSPF, Network Area.

2. Select Show Process from the Action list.

**Figure 23: Showing OSPF Process Identifiers**



## CONFIGURING GENERAL PROTOCOL SETTINGS

To implement dynamic OSPF routing, first assign VLAN groups to each IP subnet to which this router will be attached (as described in the preceding section), then use the Routing Protocol > OSPF > System (Configure) page to assign an Router ID to this device, and set the other basic protocol parameters.

### CLI REFERENCES

■"Open Shortest Path First (OSPFv2)" on page 1138

### PARAMETERS

These parameters are displayed in the web interface:

■**Process ID** – Protocol identifier as configured on the Routing Protocol > OSPF > Network Area (Add) page. (Range: 1-65535)

*General Information*

■**RFC1583 Compatible** – If one or more routers in a routing domain are using early Version 2 of OSPF, this router should use RFC 1583 (early OSPFv2) compatibility mode to ensure that all routers are using the same RFC for calculating summary route costs. Enable this field to force the router to calculate summary route costs using RFC 1583. (Default: Disabled)

When RFC 1583 compatibility is enabled, only cost is used when choosing among multiple AS-external LSAs advertising the same destination. When disabled, preference is based on type of path, using cost only to break ties (see RFC 2328).

If there any OSPF routers in an area exchanging summary information (specifically, ABRs) which have not been upgraded to OSPFv2 (RFC 2328), RFC 1583 should be used on the newly upgraded OSPFv2 routers to ensure compatibility with routers still running older OSPFv2 code.

■**OSPF Router ID** – Assigns a unique router ID for this device within the autonomous system for the current OSPF process.

The router ID must be unique for every router in the autonomous system. Also, note that the router ID can be set to 255.255.255.255.

If this router already has registered neighbors, the new router ID will be used when the router is rebooted, or manually restarted using the no router ospf command followed by the router ospf command.

■**Auto Cost** – Calculates the cost for an interface by dividing the reference bandwidth by the interface bandwidth. The reference bandwidth is defined in Mbits per second. (Range: 1-4294967)

By default, the cost is 0.1 for Gigabit ports, and 0.01 for 10 Gigabit ports. A higher reference bandwidth can be used for aggregate links to indicate preferred use as a lower cost interface.

■**SPF Hold Time** – The hold time between making two consecutive shortest path first (SPF) calculations. (Range: 0-65535 seconds; Default: 10 seconds)

Setting the SPF holdtime to 0 means that there is no delay between consecutive calculations.

■**SPF Delay Time** – The delay after receiving a topology change notification and starting the SPF calculation. (Range: 0-65535 seconds; Default: 5 seconds)

Using a low value for the delay and hold time allows the router to switch to a new path faster, but uses more CPU processing time.

- **Default Metric** – The default metric for external routes imported from other protocols. (Range: 0-16777214; Default: 20)

  A default metric must be used to resolve the problem of redistributing external routes from other protocols that use incompatible metrics.

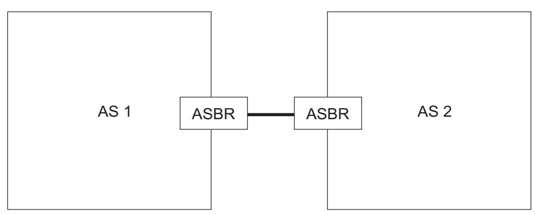
  This default metric does not override the metric value set on the Redistribute configuration screen (see page 522). When a metric value has not been configured on the Redistribute page, the default metric configured on the System configuration page sets the metric value to be used for all imported external routes.

*Default Information*

- **Originate Default Route**[1] – Generates a default external route into an autonomous system. Note that the **Advertise Default Route** field must also be properly configured. (Default: Disabled)

  When this feature is used to redistribute routes into a routing domain (that is, an Autonomous System), this router automatically becomes an Autonomous System Boundary Router (ASBR). This allows the router to exchange routing information with boundary routers in other autonomous systems to which it may be attached. If a router is functioning as an ASBR, then every other router in the autonomous system can learn about external routes from this device.

**Figure 24: AS Boundary Router**




- **Advertise Default Route**[1] – The router can advertise a default external route into the autonomous system (AS). (Options: Not Always, Always; Default: Not Always)

  - **Always** – The router will advertise itself as a default external route for the local AS, even if a default external route does not actually exist. (To define a default route, see "Configuring Static Routes" on page 449.)

  - **NotAlways** – It can only advertise a default external route into the AS if it has been configured to import external routes through RIP or static routes, and such a route is known. (See "Redistributing External Routes" on page 522.)

- **External Metric Type**[1] – The external link type used to advertise the default route. Type 1 route advertisements add the internal cost to the external route metric. Type 2 routes do not add the internal cost metric. When comparing Type 2 routes, the internal cost is only used as a tie-breaker if several Type 2 routes have the same cost. (Default: Type 2)

1. These are configured with the default-information originate command.

■ **Default External Metric**[1] – Metric assigned to the default route. (Range: 0-16777215; Default: 20)

The metric for the default external route is used to calculate the path cost for traffic passed from other routers within the AS out through the ASBR.

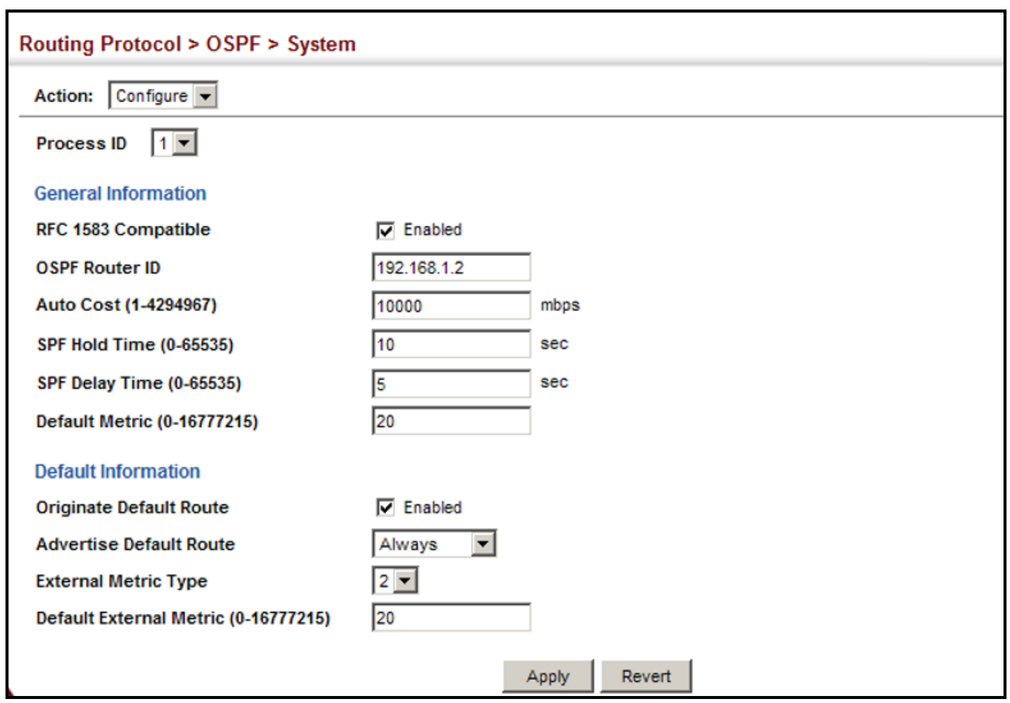
Redistribution of routing information from other protocols is controlled by the Redistribute function (see page 522).

### WEB INTERFACE

To configure general settings for OSPF:

1. Click Routing Protocol, OSPF, System.
2. Select Configure from the Action list.
3. Select a Process ID, and then specify the Router ID and other global attributes as required. For example, by setting the Auto Cost to 10000, the cost of using an interface is set to 10 for Gigabit ports, and 1 for 10 Gigabit ports.
4. Click Apply

**Figure 25: Configure General Settings for OSPF**




## DISPLAYING ADMINISTRATIVE SETTINGS AND STATISTICS

Use the Routing Protocol > OSPF > System (Show) page to display general administrative settings and statistics for OSPF.

### CLI REFERENCES

- "show ip ospf" on page 1162
- "show ip protocols ospf" on page 1175

### PARAMETERS

These parameters are displayed in the web interface:

**Table 1: OSPF System Information**

| Parameter | Description |
|---|---|
| Router ID Type | Indicates if the router ID was manually configured or automatically generated by the system. |
| Rx LSAs | The number of link-state advertisements that have been received. |
| Originate LSAs | The number of new link-state advertisements that have been originated. |
| AS LSA Count | The number of autonomous system LSAs in the link-state database. |
| External LSA Count | The number of external link-state advertisements in the link-state database. |
| External LSA Checksum | Checksum of the external link-state advertisement database. |
| Admin Status | Indicates if there are one or more configured OSPF areas with an active interface (that is, a Layer 3 interface that is enabled and up). |
| ABR Status (Area Border Router) | Indicates if this router connects directly to networks in two or more areas. An area border router runs a separate copy of the Shortest Path First algorithm, maintaining a separate routing database for each area. |
| ASBR Status (Autonomous System Boundary Router) | Indicates if this router exchanges routing information with boundary routers in other autonomous systems to which it may be attached. If a router is enabled as an ASBR, then every other router in the autonomous system can learn about external routes from this device. |
| Restart Status | Indicates if the OSPF process is in graceful-restart state. |
| Area Number | The number of configured areas attached to this router. |
| Version Number | The OSPF version number. The OSPF protocol implemented in this device is based on RFC 2328 (Version 2). It also supports RFC 1583 (early Version 2) compatibility mode. |

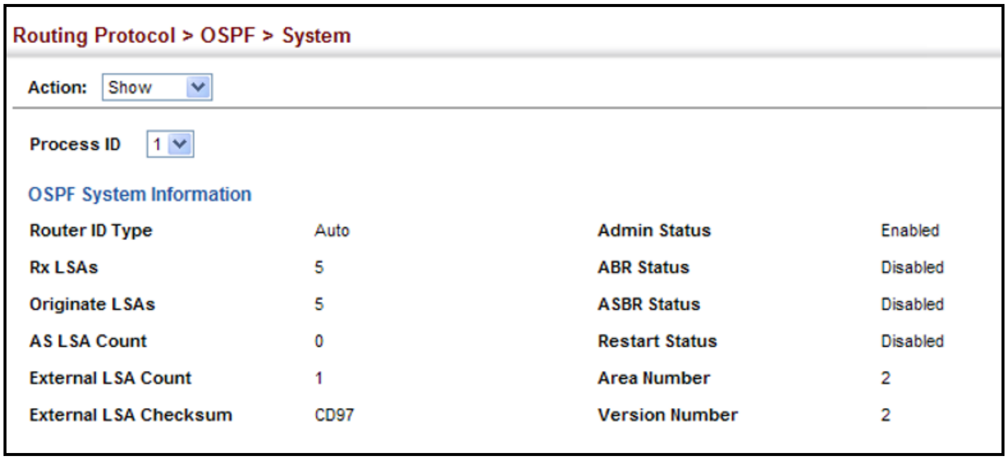
### WEB INTERFACE

To show administrative settings and statistics for OSPF:

To display general settings for OSPF:

1. Click Routing Protocol, OSPF, System.
2. Select Show from the Action list.
3. Select a Process ID.

**Figure 26: Showing General Settings for OSPF**




## ADDING AN NSSA OR STUB

Use the Routing Protocol > OSPF > Area (Configure Area – Add Area) page to add a not-so-stubby area (NSSA) or a stubby area (Stub).

### CLI REFERENCES

■"router ospf" on page 1139
■"area stub" on page 1150
■"area nssa" on page 1149

### COMMAND USAGE

■This router supports up to 5 stubs or NSSAs.

### PARAMETERS

These parameters are displayed in the web interface:

■**Process ID** – Protocol identifier as configured on the Routing Protocol > OSPF > Network Area (Add) page. (Range: 1-65535)

■**Area ID** – Identifier for a not-so-stubby area (NSSA) or stub. The area ID can be in the form of an IPv4 address, or as a four octet unsigned integer ranging from 0-4294967295.

Set the area ID to the same value for all routers on a network segment using the network mask to add one or more interfaces to an area.

■**Area Type** – Specifies an NSSA or stub.

### WEB INTERFACE

To add an NSSA or stub to the OSPF administrative domain:

1. Click Routing Protocol, OSPF, Area.

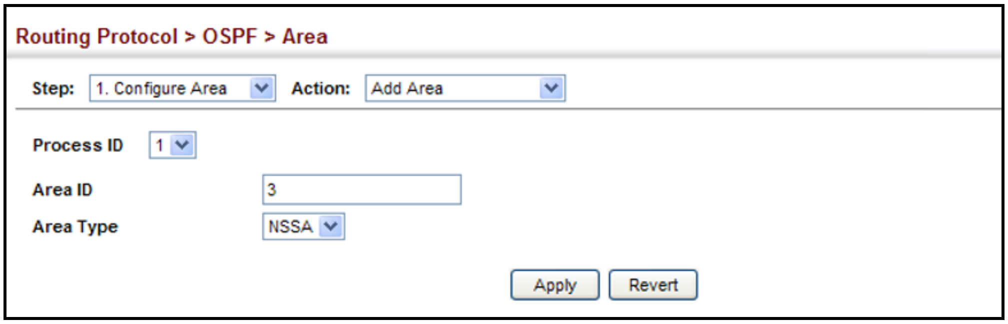
2. Select Configure Area from the Step list.

3. Select Add Area from the Action list.

4. Select a Process ID, enter the area identifier, and set the area type to NSSA or Stub.

5. Click Apply

**Figure 27: Adding an NSSA or Stub**




To show the NSSA or stubs added to the specified OSPF domain:

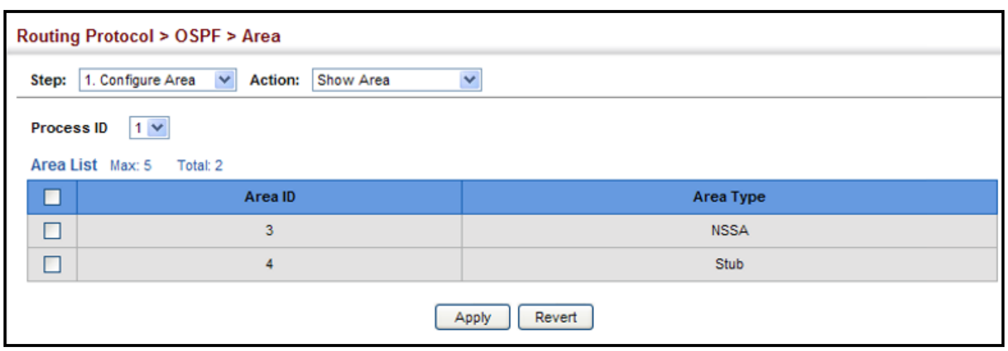
1. Click Routing Protocol, OSPF, Area.

2. Select Configure Area from the Step list.

3. Select Show Area from the Action list.

4. Select a Process ID.

**Figure 28: Showing NSSAs or Stubs**




## CONFIGURING NSSA SETTINGS

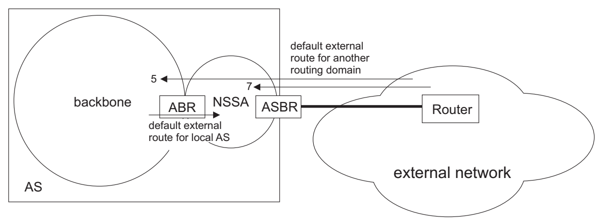
Use the Routing Protocol > OSPF > Area (Configure Area – Configure NSSA Area) page to configure protocol settings for a not-so-stubby area (NSSA).

An NSSA can be configured to control the use of default routes for Area Border Routers (ABRs) and Autonomous System Boundary Routers (ASBRs), or external routes learned from other routing domains and imported through an ABR.

An NSSA is similar to a stub. It blocks most external routing information, and can be configured to advertise a single default route for traffic passing between the NSSA and other areas within the autonomous system (AS) when the router is an ABR.

An NSSA can also import external routes from one or more small routing domains that are not part of the AS, such as a RIP domain or locally configured static routes. This external AS routing information is generated by the NSSA's ASBR and advertised only within the NSSA. By default, these routes are not flooded onto the backbone or into any other area by ABRs. However, the NSSA's ABRs will convert NSSA external LSAs (Type 7) into external LSAs (Type-5) which are propagated into other areas within the AS.

**Figure 29: OSPF NSSA**




### CLI REFERENCES


- "router ospf" on page 1139
- "area default-cost" on page 1144
- "area nssa" on page 1149


### COMMAND USAGE

- Before creating an NSSA, first specify the address range for the area (see "Defining Network Areas Based on Addresses" on page 506). Then create an NSSA as described under "Adding an NSSA or Stub" on page 513.

- NSSAs cannot be used as a transit area, and should therefore be placed at the edge of the routing domain.

- An NSSA can have multiple ABRs or exit points. However, all of the exit points and local routers must contain the same external routing data so that the exit point does not need to be determined for each external destination.

- There are no external routes in an OSPF stub area, so routes cannot be redistributed from another protocol into a stub area. On the other hand, an NSSA allows external routes from another protocol to be redistributed into its own area, and then leaked to adjacent areas.

- Routes that can be advertised with NSSA external LSAs include network destinations outside the AS learned through OSPF, the default route, static routes, routes derived from other routing protocols such as RIP, or directly connected networks that are not running OSPF.

- An NSSA can be used to simplify administration when connecting a central site using OSPF to a remote site that is using a different routing protocol. OSPF can be easily extended to cover the remote connection by defining the area between the central router and the remote router as an NSSA.

### PARAMETERS

These parameters are displayed in the web interface:

- **Process ID** – Process ID as configured in the Network Area configuration screen (see page 506).

- **Area ID** – Identifier for a not-so-stubby area (NSSA).
- **Translator Role** – Indicates NSSA-ABR translator role for converting Type 7 external LSAs into Type 5 external LSAs. These roles include:
  - **Never** – A router that never translates NSSA LSAs to Type-5 external LSAs.
  - **Always** – A router that always translates NSSA LSA to Type-5 external LSA.
  - **Candidate** – A router translates NSSA LSAs to Type-5 external LSAs if elected.
- **Redistribute** – Disable this option when the router is an NSSA Area Border Router (ABR) and routes only need to be imported into normal areas (see "Redistributing External Routes" on page 522), but not into the NSSA. In other words, redistribution should be disabled to prevent the NSSA ABR from advertising external routing information (learned through routers in other areas) into the NSSA. (Default: Enabled)
- **Originate Default Information** – When the router is an NSSA Area Border Router (ABR) or an NSSA Autonomous System Boundary Router (ASBR), this option causes it to generate a Type-7 default LSA into the NSSA. This default provides a route to other areas within the AS for an NSSA ABR, or to areas outside the AS for an NSSA ASBR. (Default: Disabled)

  An NSSA is similar to a stub, because when the router is an ABR, it can send a default route for other areas in the AS into the NSSA using the Originate Default Information option. However, an NSSA is different from a stub, because when the router is an ASBR, it can import a default external AS route (for routing protocol domains adjacent to the NSSA but not within the OSPF AS) into the NSSA using this option.
- **Metric Type** – Type 1 or Type 2 external routes. When using Type 2, routers do not add internal cost to the external route metric. (Default: Type 2)
- **Metric** – Metric assigned to Type-7 default LSAs. (Range: 1-16777214; Default: 1)
- **Default Cost** – Cost for the default summary route sent into an NSSA from an area border router (ABR). (Range: 0-16777215; Default: 0)

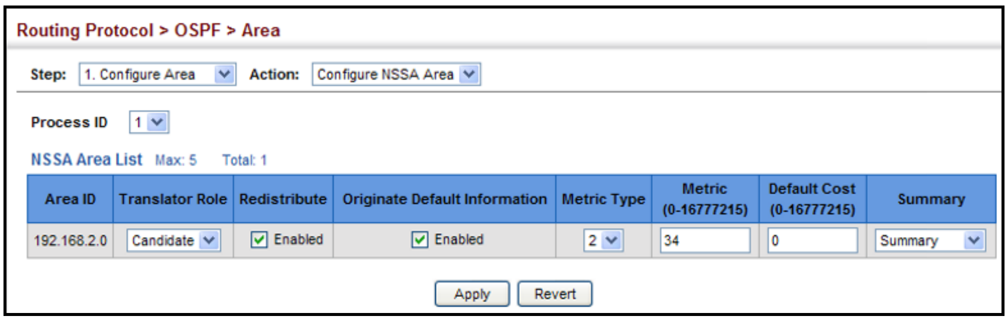
  Note that when the default cost is set to “0,” the router will not advertise a default route into the attached NSSA.
- **Summary** – Controls the use of summary routes. (Default: Summary)
  - **Summary** – Unlike stub areas, all Type-3 summary LSAs will be imported into NSSAs to ensure that internal routes are always chosen over Type-7 NSSA external routes.
  - **No Summary** – Allows an area to retain standard NSSA features, but does not inject inter-area routes (Type-3 and Type-4 summary routes) into this area. Instead, it advertises a default route as a Type-3 LSA.

#### WEB INTERFACE

To configure protocol settings for an NSSA:

1. Click Routing Protocol, OSPF, Area.
2. Select Configure Area from the Step list.
3. Select Configure NSSA Area from the Action list.
4. Select a Process ID, and modify the routing behavior for an NSSA.
5. Click Apply

**Figure 30: Configuring Protocol Settings for an NSSA**

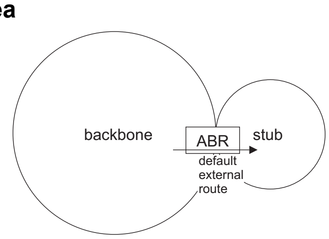



### CONFIGURING STUB SETTINGS

Use the Routing Protocol > OSPF > Area (Configure Area – Configure Stub Area) page to configure protocol settings for a stub.

A stub does not accept external routing information. Instead, an area border router adjacent to a stub can be configured to send a default external route into the stub for all destinations outside the local area or the autonomous system. This route will also be advertised as a single entry point for traffic entering the stub. Using a stub can significantly reduce the amount of topology data that has to be exchanged over the network.

**Figure 31: OSPF Stub Area**




By default, a stub can only pass traffic to other areas in the autonomous system through the default external route. However, an area border router can also be configured to send Type 3 summary link advertisements into the stub about subnetworks located elsewhere in the autonomous system.

### CLI REFERENCES

- "router ospf" on page 1139
- "area default-cost" on page 1144
- "area stub" on page 1150

### COMMAND USAGE

- Before creating a stub, first specify the address range for the area (see "Defining Network Areas Based on Addresses" on page 506). Then create a stub as described under "Adding an NSSA or Stub" on page 513.
- Stubs cannot be used as a transit area, and should therefore be placed at the edge of the routing domain.
- A stub can have multiple ABRs or exit points. However, all of the exit points and local routers must contain the same external routing data so that the exit point does not need to be determined for each external destination.

### PARAMETERS

These parameters are displayed in the web interface:

- **Process ID** – Process ID as configured in the Network Area configuration screen (see page 506).
- **Area ID** – Identifier for a stub.
- **Default Cost** – Cost for the default summary route sent into a stub from an area border router (ABR). (Range: 0-16777215; Default: 0)

  Note that he the default cost is set to “0,” the router will not advertise a default route into the attached stub.
- **Summary** – Controls the use of summary routes.
  - **Summary** – Allows an Area Border Router (ABR) to send a summary link advertisement into the stub area.
  - **No Summary** – Stops an ABR from sending a summary link advertisement into a stub area.

    Routing table space is saved in a stub by blocking Type-4 AS summary LSAs and Type 5 external LSAs. This option can be used to completely isolate the stub by also stopping an ABR from sending Type-3 summary LSAs that advertise the default route for destinations external to the local area or the autonomous system.

    Define an area as a totally stubby area only if routers in the area do not require summary LSAs from other areas.

### WEB INTERFACE

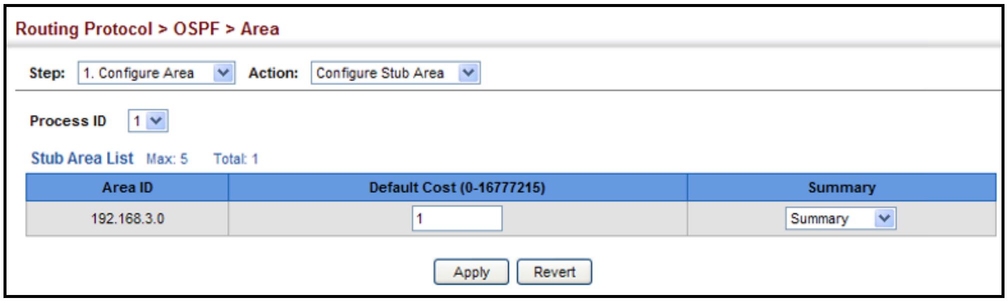
To configure protocol settings for a stub:

1. Click Routing Protocol, OSPF, Area.
2. Select Configure Area from the Step list.
3. Select Configure Stub Area from the Action list.

**4.** Select a Process ID, and modify the routing behavior for a stub.

**5.** Click Apply

**Figure 32: Configuring Protocol Settings for a Stub**




## DISPLAYING INFORMATION ON NSSA AND STUB AREAS

Use the Routing Protocol > OSPF > Area (Show Information) page to protocol information on NSSA and Stub areas.

### CLI REFERENCES

■ "show ip ospf" on page 1162

### PARAMETERS

These parameters are displayed in the web interface:

■ **Process ID** – Process ID as configured in the Network Area configuration screen (see page 506).

■ **Area ID** – Identifier for a not-so-stubby area (NSSA) or stub.

■ **SPF Runs** – The number of times the Shortest Path First algorithm has been run for this area.

■ **ABR Count** – The number of Area Border Routers attached to this area.

■ **ASBR Count** – The number of Autonomous System Boundary Routers attached to this area.

■ **LSA Count** – The number of new link-state advertisements that have been originated.

■ **LSA Checksum Sum** – The sum of the link-state advertisements' LS checksums contained in this area's link-state database.

### WEB INTERFACE

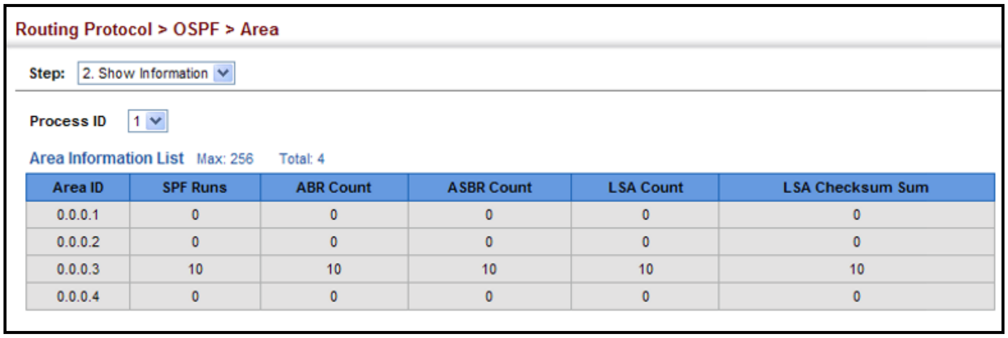
To display information on NSSA and stub areas:

**1.** Click Routing Protocol, OSPF, Area.

**2.** Select Show Information from the Action list.

**3.** Select a Process ID.

**Figure 33: Displaying Information on NSSA and Stub Areas**



Routing Protocol > OSPF > Area

Step: 2. Show Information

Process ID 1

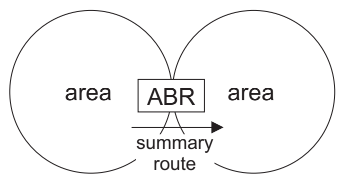
Area Information List Max: 256 Total: 4

| Area ID | SPF Runs | ABR Count | ASBR Count | LSA Count | LSA Checksum Sum |
|---|---|---|---|---|---|
| 0.0.0.1 | 0 | 0 | 0 | 0 | 0 |
| 0.0.0.2 | 0 | 0 | 0 | 0 | 0 |
| 0.0.0.3 | 10 | 10 | 10 | 10 | 10 |
| 0.0.0.4 | 0 | 0 | 0 | 0 | 0 |

## CONFIGURING AREA RANGES (ROUTE SUMMARIZATION FOR ABRS)

An OSPF area can include a large number of nodes. If the Area Border Router (ABR) has to advertise route information for each of these nodes, this wastes a lot of bandwidth and processor time. Instead, you can use the Routing Protocol > OSPF > Area Range (Add) page to configure an ABR to advertise a single summary route that covers all the individual networks within its area. When using route summaries, local changes do not have to be propagated to other area routers. This allows OSPF to be easily scaled for larger networks, and provides a more stable network topology.

**Figure 34: Route Summarization for ABRs**




### CLI REFERENCES

- "router ospf" on page 1139
- "area range" on page 1144

### COMMAND USAGE

- Use the Area Range configuration page to summarize intra-area routes, and advertise this information to other areas through Area Border Routers (ABRs). The summary route for an area is defined by an IP address and network mask. You therefore need to structure each area with a contiguous set of addresses so that all routes in the area fall within an easily specified range. If it is not possible to use one contiguous set of addresses, then the routes can be summarized for several area ranges.This router also supports Variable Length Subnet Masks (VLSMs), so you can summarize an address range on any bit boundary in a network address.

- To summarize the external LSAs imported into your autonomous system (i.e., local routing domain), use the Summary Address configuration screen (page 520).

- This router supports up five summary routes for area ranges.

### PARAMETERS

These parameters are displayed in the web interface:

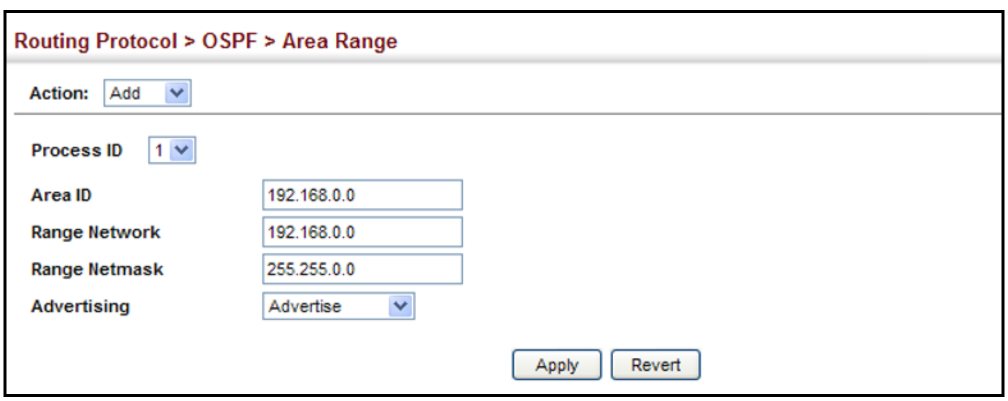
- **Process ID** – Process ID as configured in the Network Area configuration screen (see page 506).
- **Area ID** – Identifies an area for which the routes are summarized. The area ID can be in the form of an IPv4 address, or also as a four octet unsigned integer ranging from 0-4294967295.
- **Range Network** – Base address for the routes to summarize.
- **Range Netmask** – Network mask for the summary route.
- **Advertising** – Indicates whether or not to advertise the summary route. If the routes are set to be advertised, the router will issue a Type 3 summary LSA for each specified address range. If the summary is not advertised, the specified routes remain hidden from the rest of the network. (Default: Advertise)

### WEB INTERFACE

To configure a route summary for an area range:

1. Click Routing Protocol, OSPF, Area Range.
2. Select Add from the Action list.
3. Specify the process ID, area identifier, the base address and network mask, and select whether or not to advertise the summary route to other areas.
4. Click Apply

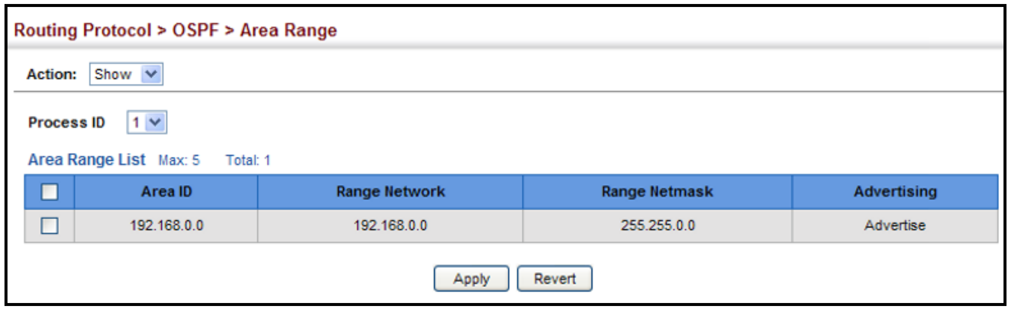
**Figure 35: Configuring Route Summaries for an Area Range**




To show the configured route summaries:

1. Click Routing Protocol, OSPF, Area Range.
2. Select Show from the Action list.
3. Select the process ID.

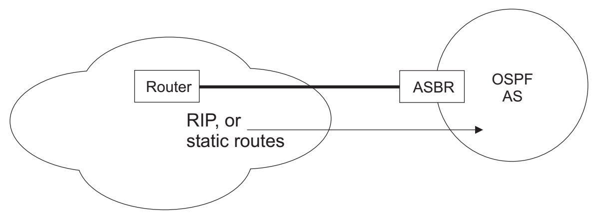
**Figure 36: Showing Configured Route Summaries**




## REDISTRIBUTING EXTERNAL ROUTES

Use the Routing Protocol > OSPF > Redistribute (Add) page to import external routing information from other routing protocols, static routes, or directly connected routes into the autonomous system, and to generate AS-external-LSAs.

**Figure 37: Redistributing External Routes**




### CLI REFERENCES

- "router ospf" on page 1139
- "redistribute" on page 1184

### COMMAND USAGE

- This router supports redistribution for all currently connected routes, entries learned through RIP, and static routes.
- When you redistribute external routes into an OSPF autonomous system (AS), the router automatically becomes an autonomous system boundary router (ASBR).
- However, if the router has been configured as an ASBR via the General Configuration screen, but redistribution is not enabled, the router will only generate a “default” external route into the AS if it has been configured to “always” advertise a default route even if an external route does not actually exist (page 509).

### PARAMETERS

These parameters are displayed in the web interface:

- **Process ID** – Process ID as configured in the Network Area configuration screen (see page 506).
- **Protocol Type** – Specifies the external routing protocol type for which routing information is to be redistributed into the local routing domain. (Options: RIP, Static; Default: RIP)

- **Metric Type** – Indicates the method used to calculate external route costs. (Options: Type 1, Type 2; Default: Type 1)

  Metric type specifies the way to advertise routes to destinations outside the autonomous system (AS) through External LSAs. Specify Type 1 to add the internal cost metric to the external route metric. In other words, the cost of the route from any router within the AS is equal to the cost associated with reaching the advertising ASBR, plus the cost of the external route. Specify Type 2 to only advertise the external route metric.

- **Metric** – Metric assigned to all external routes for the specified protocol. (Range: 1-65535: Default: 10)

  The metric value specified for redistributed routes supersedes the Default External Metric specified in the Routing Protocol > OSPF > System screen (page 509).

- **Tag** – A tag placed in the AS-external LSA to identify a specific external routing domain, or to pass additional information between routers. (Range: 0-4294967295)

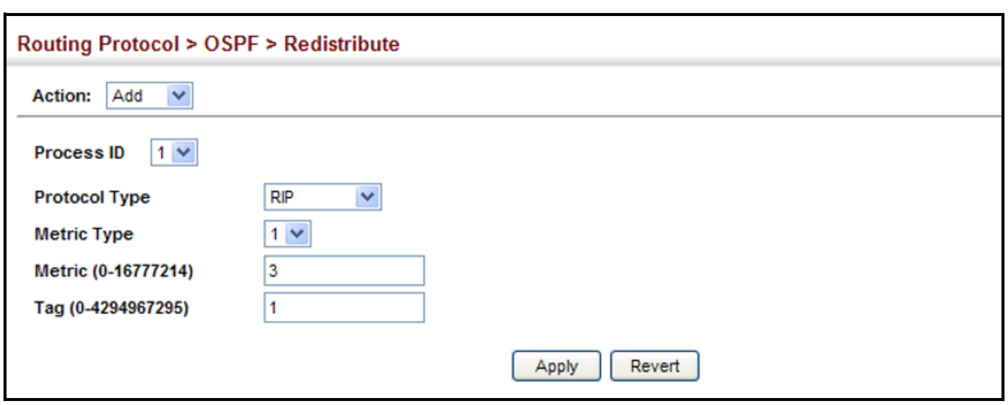
  A tag can be used to distinguish between routes learned from different external autonomous systems (other routing protocols). For example, if there are two ASBRs in a routing domain: A and B. ASBR A can be configured to redistribute routes learned from RIP domain 1 (identified by tag 1) and ASBR B can redistribute routes learned from RIP domain 2 (identified by tag 2).

### WEB INTERFACE

To configure the router to import external routing information:

1. Click Routing Protocol, OSPF, Redistribute.
2. Select Add from the Action list.
3. Specify the process ID, the protocol type to import, the metric type, path cost, and optional tag.
4. Click Apply.

**Figure 38: Importing External Routes**



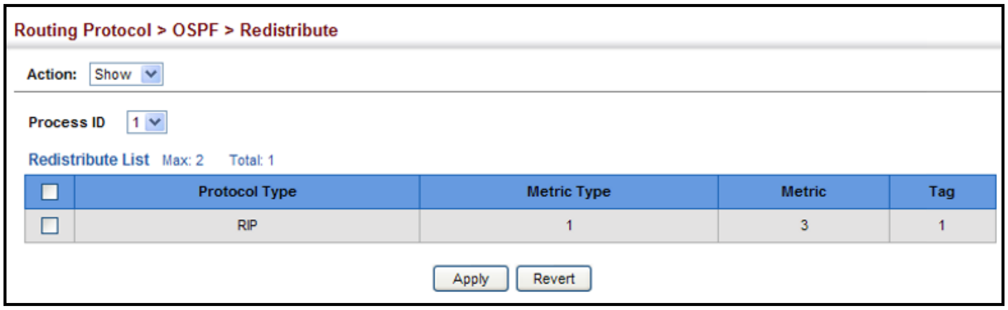

To show the imported external route types:

1. Click Routing Protocol, OSPF, Redistribute.

2. Select Show from the Action list.

3. Select the process ID.

**Figure 39: Showing Imported External Route Types**




## CONFIGURING SUMMARY ADDRESSES (FOR EXTERNAL AS ROUTES)

Redistributing routes from other protocols into OSPF normally requires the router to advertise each route individually in an external LSA as described in the preceding section. The reduce the number of protocol messages required to redistribute these external routes, an Autonomous System Boundary Router (ASBR) can instead be configured to redistribute routes learned from other protocols into all attached autonomous systems.

To reduce the amount of external LSAs sent to other autonomous systems, you can use the Routing Protocol > OSPF > Summary Address (Add) page to configure the router to advertise an aggregate route that consolidates a broad range of external addresses. This helps both to decrease the number of external LSAs advertised and the size of the OSPF link state database.

### CLI REFERENCES

- "router ospf" on page 1139
- "summary-address" on page 1148

### COMMAND USAGE

- If you are not sure what address ranges to consolidate, first enable external route redistribution via the Redistribute configuration screen, view the routes imported into the routing table, and then configure one or more summary addresses to reduce the size of the routing table and consolidate these external routes for advertising into the local domain.

- To summarize routes sent between OSPF areas, use the Area Range Configuration screen (page 520).

- This router supports up 20 Type-5 summary routes.

### PARAMETERS

These parameters are displayed in the web interface:

- **Process ID** – Process ID as configured in the Network Area configuration screen (see page 506).

- **IP Address** – Summary address covering a range of addresses.

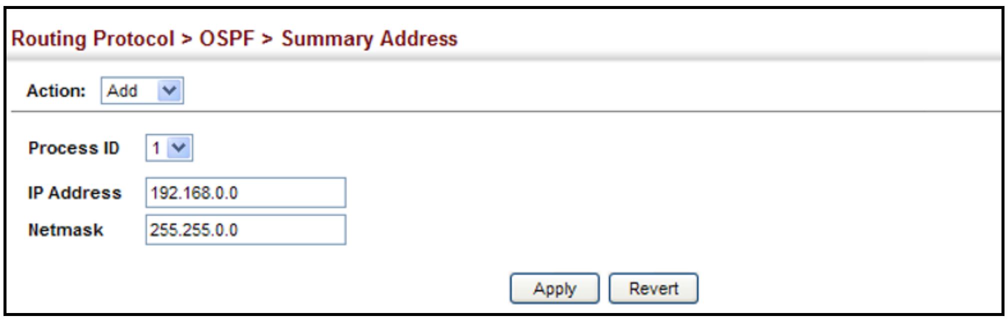
- **Netmask** – Network mask for the summary route.

### WEB INTERFACE

To configure the router to summarize external routing information:

1. Click Routing Protocol, OSPF, Summary Address.
2. Select Add from the Action list.
3. Specify the process ID, the base address and network mask.
4. Click Apply.

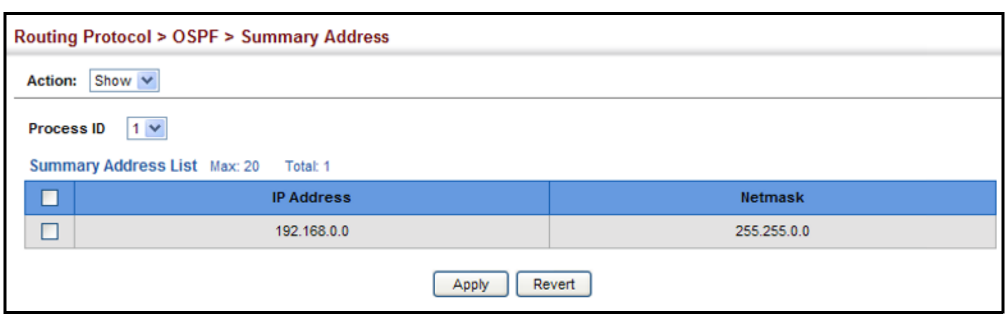
**Figure 40: Summarizing External Routes**




To show the summary addresses for external routes:

1. Click Routing Protocol, OSPF, Summary Address.
2. Select Show from the Action list.
3. Select the process ID.

**Figure 41: Showing Summary Addresses for External Routes**




## CONFIGURING OSPF INTERFACES

You should specify a routing interface for any local subnet that needs to communicate with other network segments located on this router or elsewhere in the network. First configure a VLAN for each subnet that will be directly connected to this router, assign IP interfaces to each VLAN (i.e., one primary interface and one or more secondary interfaces), and then use the Network Area configuration page to assign an interface address range to an OSPF area.

After assigning a routing interface to an OSPF area, use the Routing Protocol > OSPF > Interface (Configure by VLAN) or (Configure by Address) page to configure the interface-specific parameters used by OSPF to set the cost used to select preferred paths, select the designated router, control the timing of link state advertisements, and specify the method used to authenticate routing messages.

### CLI REFERENCES

- "Open Shortest Path First (OSPFv2)" on page 1138

### COMMAND USAGE

- The Configure by VLAN page is used to set the OSPF interface settings for the all areas assigned to a VLAN on the Network Area (Add) page (see page 506).
- The Configure by Address page is used to set the OSPF interface settings for a specific area assigned to a VLAN on the Network Area (Add) page (see page 506).

### PARAMETERS

These parameters are displayed in the web interface:

- **VLAN ID** – A VLAN to which an IP interface has been assigned.
- **IP Address** – Address of the interfaces assigned to a VLAN on the Network Area (Add) page.

  This parameter only applies to the Configure by Address page.
- **Cost** – Sets the cost of sending a protocol packet on an interface, where higher values indicate slower ports. (Range: 1-65535; Default: 1)

  The interface cost indicates the overhead required to send packets across a certain interface. This is advertised as the link cost in router link state advertisements.

  Routes are assigned a metric equal to the sum of all metrics for each interface link in the route.

  This router uses a default cost of 1 for all ports. Therefore, if you install a 10 Gigabit module, you need to reset the cost for all of the 1 Gbps ports to a value greater than 1 to reflect the actual interface bandwidth.
- **Router Priority** – Sets the interface priority for this router. (Range: 0-255; Default: 1)

  This priority determines the designated router (DR) and backup designated router (BDR) for each OSPF area. The DR forms an active adjacency to all other routers in the area to exchange routing topology information. If for any reason the DR fails, the BDR takes over this role.

  Set the priority to zero to prevent a router from being elected as a DR or BDR. If set to any value other than zero, the router with the highest priority becomes the DR and the router with the next highest priority becomes the BDR. If two or more routers are set to the same highest priority, the router with the higher ID will be elected.

If a DR already exists for an area when this interface comes up, the new router will accept the current DR regardless of its own priority. The DR will not change until the next time the election process is initiated.

Configure router priority for multi-access networks only and not for point-to-point networks.

- **Hello Interval** – Sets the interval between sending hello packets on an interface. This interval must be set to the same value for all routers on the network. (Range: 1-65535 seconds; Default: 10)

  Hello packets are used to inform other routers that the sending router is still active. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase routing traffic.

- **Dead Interval** – Sets the interval at which hello packets are not seen before neighbors declare the router down. This interval must be set to the same value for all routers on the network. (Range: 1-65535 seconds; Default: 40, or 4 times the Hello Interval)

  The dead-interval is advertised in the router's hello packets. It must be a multiple of hello-interval and be the same for all routers on a specific network.

- **Transmit Delay** – Sets the estimated time to send a link-state update packet over an interface. (Range: 1-65535 seconds; Default: 1 second)

  LSAs have their age incremented by this delay before transmission. You should consider both the transmission and propagation delays for an interface when estimating this delay. Set the transmit delay according to link speed, using larger values for lower-speed links.

  If this delay is not added, the time required to transmit an LSA over the link is not taken into consideration by the routing process. On slow links, the router may send packets more quickly than devices can receive them. To avoid this problem, you can use the transmit delay to force the router to wait a specified interval between transmissions.

- **Retransmit Interval** – Sets the time between resending link-state advertisements. (Range: 1-65535 seconds; Default: 5 seconds)

  A router will resend an LSA to a neighbor if it receives no acknowledgment after the specified retransmit interval. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. Note that this value should be larger for virtual links.

  Set this interval to a value that is greater than the round-trip delay between any two routers on the attached network to avoid unnecessary retransmissions.

- **Authentication Type** – Specifies the authentication type used for an interface. (Options: None, Simple, MD5; Default: None)

  Use authentication to prevent routers from inadvertently joining an unauthorized area. Configure routers in the same area with the same password (or key). All neighboring routers on the same network with the same password will exchange routing data.

  When using simple password authentication, a password is included in the packet. If it does not match the password configured on the receiving router, the packet is discarded. This method provides very little security as it is possible to learn the authentication key by snooping on routing protocol packets.

When using Message-Digest 5 (MD5) authentication, the router uses the MD5 algorithm to verify data integrity by creating a 128-bit message digest from the authentication key. Without the proper key and key-id, it is nearly impossible to produce any message that matches the prespecified target message digest.

The Message Digest Key ID and Authentication Key and must be used consistently throughout the autonomous system.

- **Authentication Key** – Assign a plain-text password used by neighboring routers to verify the authenticity of routing protocol messages. (Range: 1-8 characters for simple password or 1-16 characters for MD5 authentication; Default: no key)

  When plain-text or Message-Digest 5 (MD5) authentication is enabled as described in the preceding item, this password (key) is inserted into the OSPF header when routing protocol packets are originated by this device.

  A different password can be assigned to each network interface, but the password must be used consistently on all neighboring routers throughout a network (that is, autonomous system). All neighboring routers in the same network with the same password will exchange routing data.

- **Message Digest Key ID** – Assigns a key identifier used in conjunction with the authentication key to verify the authenticity of routing protocol messages sent to neighboring routers. (Range: 1-255; Default: none)

  Normally, only one key is used per interface to generate authentication information for outbound packets and to authenticate incoming packets. Neighbor routers must use the same key identifier and key value.

  When changing to a new key, the router will send multiple copies of all protocol messages, one with the old key and another with the new key. Once all the neighboring routers start sending protocol messages back to this router with the new key, the router will stop using the old key. This rollover process gives the network administrator time to update all of the routers on the network without affecting the network connectivity. Once all the network routers have been updated with the new key, the old key should be removed for security reasons.

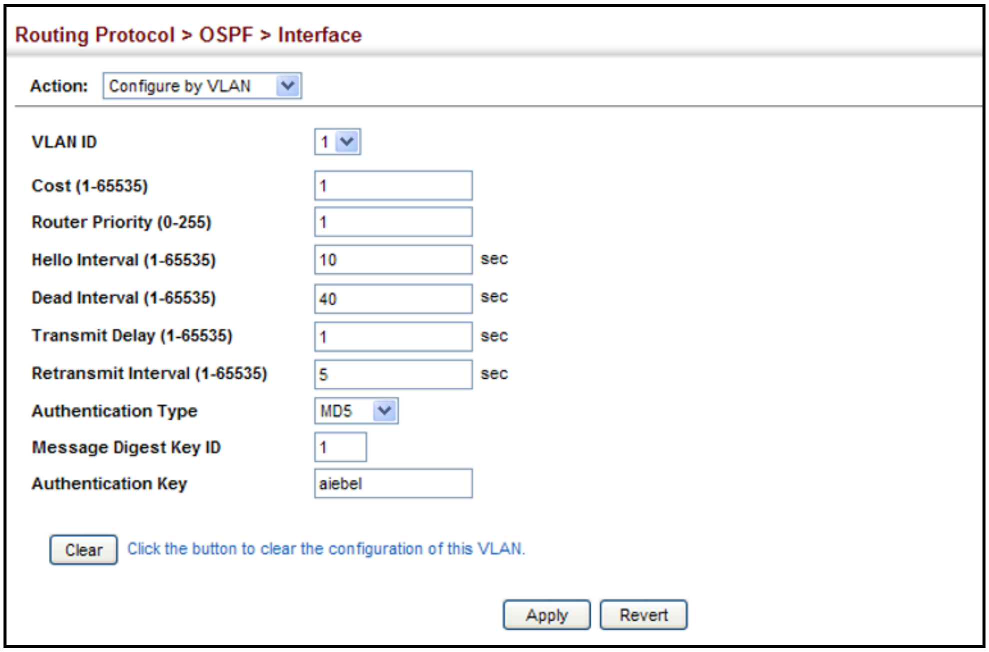
  Before setting a new key identifier, the current key must first be deleted on the Show MD5 Key page.

### WEB INTERFACE

To configure OSPF interface for all areas assigned to a VLAN:

1. Click Routing Protocol, OSPF, Interface.
2. Select Configure by VLAN from the Action list.
3. Specify the VLAN ID, and configure the required interface settings.
4. Click Apply.

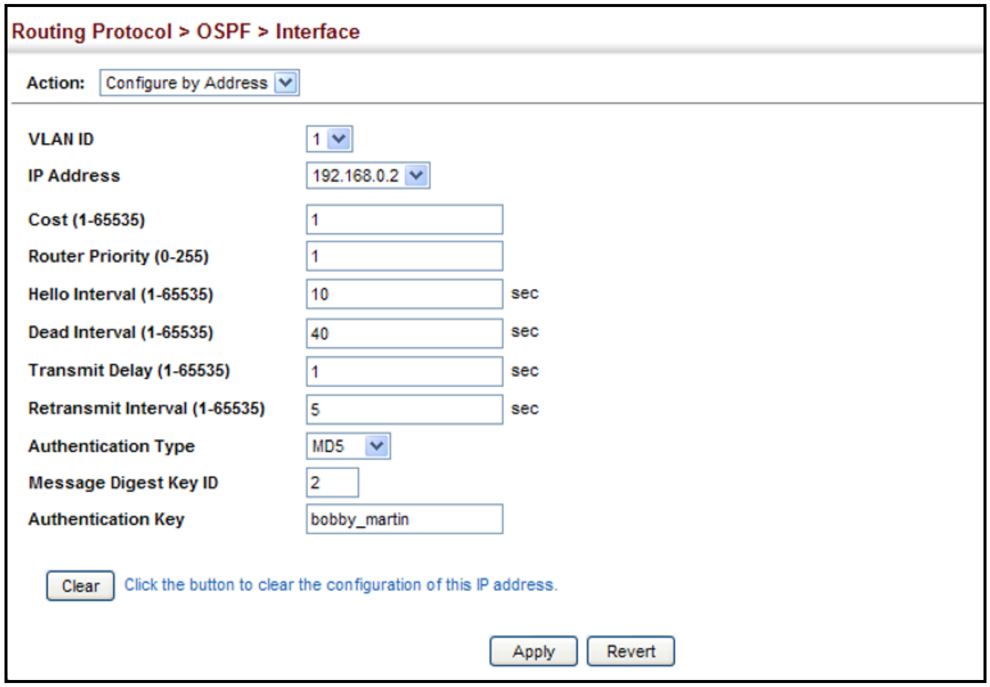
**Figure 42: Configuring Settings for All Interfaces Assigned to a VLAN**




To configure interface settings for a specific area assigned to a VLAN:

1. Click Routing Protocol, OSPF, Interface.
2. Select Configure by Address from the Action list.
3. Specify the VLAN ID, enter the address assigned to an area, and configure the required interface settings.
4. Click Apply.

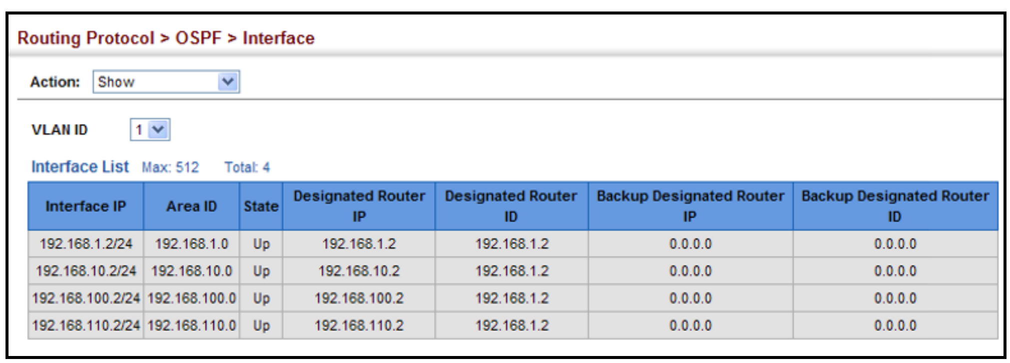
**Figure 43: Configuring Settings for a Specific Area Assigned to a VLAN**




To show the configuration settings for OSPF interfaces:

1. Click Routing Protocol, OSPF, Interface.
2. Select Show from the Action list.
3. Select the VLAN ID.

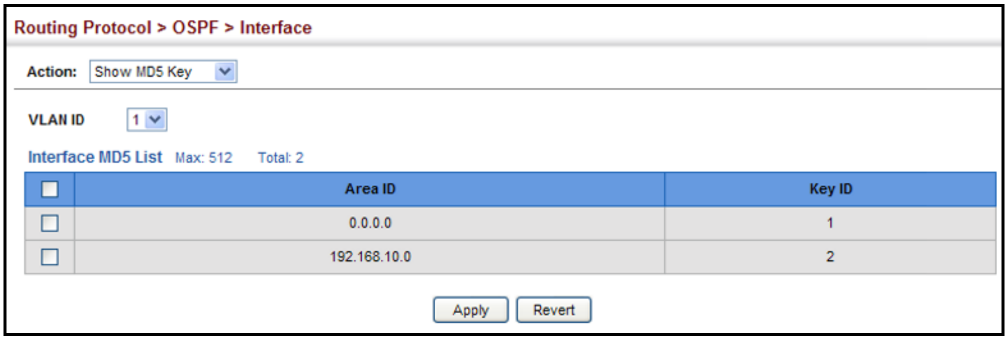
**Figure 44: Showing OSPF Interfaces**




To show the MD5 authentication keys configured for an interface:

1. Click Routing Protocol, OSPF, Interface.
2. Select Show MD5 Key from the Action list.
3. Select the VLAN ID.

**Figure 45: Showing MD5 Authentication Keys**

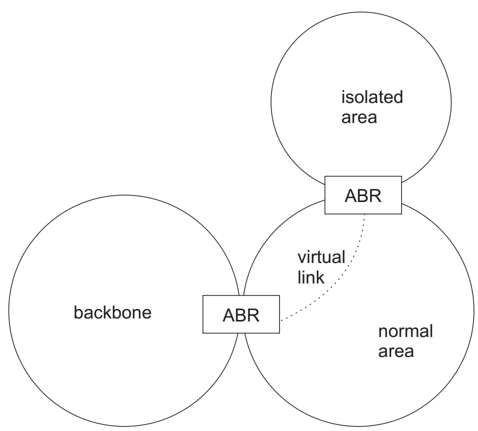



## CONFIGURING VIRTUAL LINKS

Use the Routing Protocol > OSPF > Virtual Link (Add) and (Configure Detailed Settings) pages to configure a virtual link from an area that does not have a direct physical connection to the OSPF backbone.

All OSPF areas must connect to the backbone. If an area does not have a direct physical connection to the backbone, you can configure a virtual link that provides a logical path to the backbone. To connect an isolated area to the backbone, the logical path can cross a single non-backbone area (i.e., transit area) to reach the backbone. To define this path, you must configure an ABR that serves as an endpoint connecting the isolated area to the common transit area, and specify a neighboring ABR at the other endpoint connecting the common transit area to the backbone itself. (Note that you cannot configure a virtual link that runs through a stub or NSSA.)

**Figure 46: OSPF Virtual Link**




Virtual links can also be used to create a redundant link between any area and the backbone to help prevent partitioning, or to connect two existing backbone areas into a common backbone.

Any area disconnected from the backbone must include the transit area ID and the router ID for a virtual link neighbor that is adjacent to the backbone.

This router supports up five virtual links.

### CLI REFERENCES

■ "router ospf" on page 1139

■ "area virtual-link" on page 1151

### COMMAND USAGE

■ Use the Add page to create a virtual link, and then use the Configure Detailed Settings page to set the protocol timers and authentication settings for the link. The parameters to be configured on the Configure Detailed Settings page are described under "Configuring OSPF Interfaces" on page 525.

### PARAMETERS

These parameters are displayed in the web interface:

■ **Process ID** – Process ID as configured in the Network Area configuration screen (see page 506).

■ **Area ID** – Identifies the transit area for the virtual link. The area ID must be in the form of an IPv4 address, or also as a four octet unsigned integer ranging from 0-4294967295.

■ **Neighbor** – Router ID of the virtual link neighbor. This specifies the Area Border Router (ABR) at the other end of the virtual link. To create a virtual link, it must be configured for an ABR at both ends of the link. One of the ABRs must be next to the isolated area and the transit area at one end of the link, while the other ABR must be next to the transit area and backbone at the other end of the link.

### WEB INTERFACE

To create a virtual link:

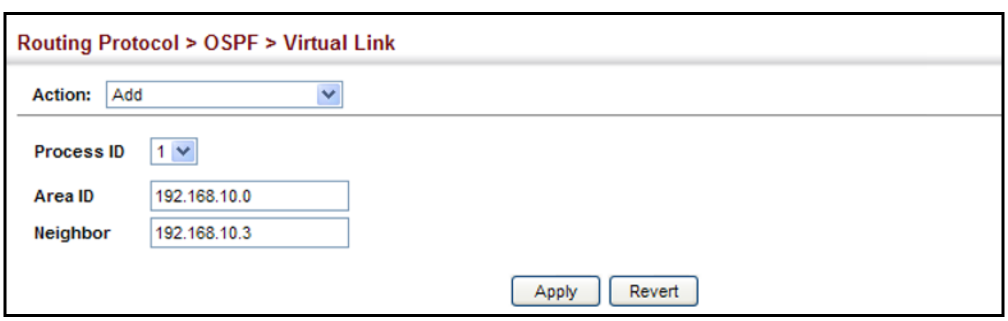
**1.** Click Routing Protocol, OSPF, Virtual Link.

**2.** Select Add from the Action list.

**3.** Specify the process ID, the Area ID, and Neighbor router ID.

**4.** Click Apply.

**Figure 47: Adding a Virtual Link**



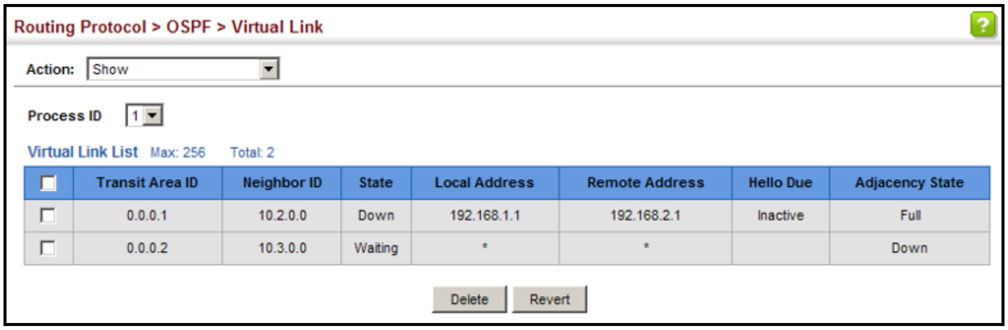

To show virtual links:

**1.** Click Routing Protocol, OSPF, Virtual Link.

**2.** Select Show from the Action list.

3. Select the process ID.

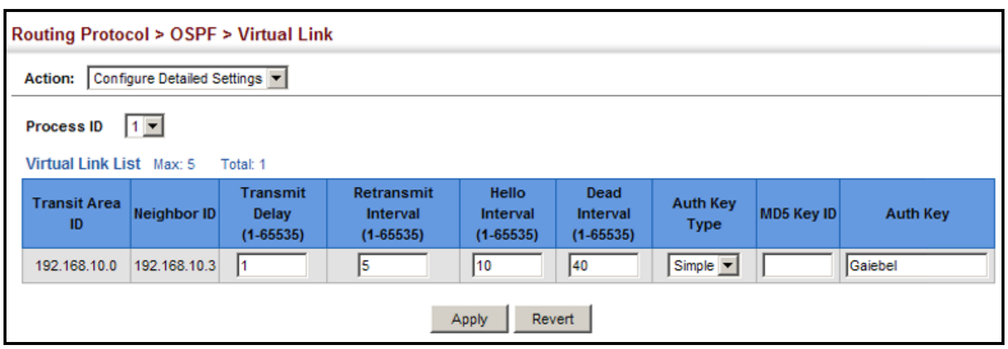
**Figure 48: Showing Virtual Links**




To configure detailed settings for a virtual link:

1. Click Routing Protocol, OSPF, Virtual Link.
2. Select Configure Detailed Settings from the Action list.
3. Specify the process ID, then modify the protocol timers and authentication settings as required.
4. Click Apply.

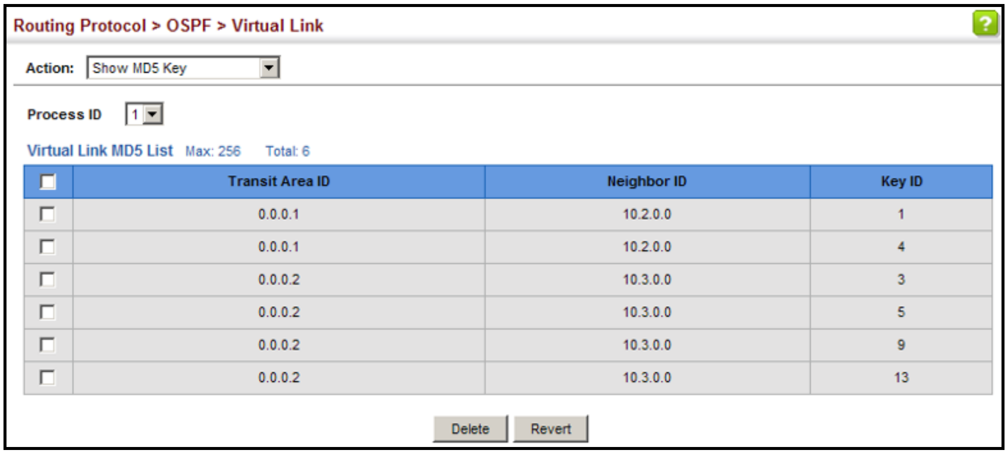
**Figure 49: Configuring Detailed Settings for a Virtual Link**




To show the MD5 authentication keys configured for a virtual link:

1. Click Routing Protocol, OSPF, Interface.
2. Select Show MD5 Key from the Action list.
3. Select the VLAN ID.

**Figure 50: Showing MD5 Authentication Keys**




## DISPLAYING LINK STATE DATABASE INFORMATION

Use the Routing Protocol > OSPF > Information (LSDB) page to show the Link State Advertisements (LSAs) sent by OSPF routers advertising routes. The full collection of LSAs collected by a router interface from the attached area is known as a link state database. Routers that are connected to multiple interfaces will have a separate database for each area. Each router in the same area should have an identical database describing the topology for that area, and the shortest path to external destinations.

The full database is exchanged between neighboring routers as soon as a new router is discovered. Afterwards, any changes that occur in the routing tables are synchronized with neighboring routers through a process called reliable flooding. You can show information about different LSAs stored in this router’s database, which may include any of the following types:

■Router (Type 1) – All routers in an OSPF area originate Router LSAs that describe the state and cost of its active interfaces and neighbors.

■Network (Type 2) – The designated router for each area originates a Network LSA that describes all the routers that are attached to this network segment.

■Summary (Type 3) – Area border routers can generate Summary LSAs that give the cost to a subnetwork located outside the area.

■AS Summary (Type 4) – Area border routers can generate AS Summary LSAs that give the cost to an autonomous system boundary router (ASBR).

■AS External (Type 5) – An ASBR can generate an AS External LSA for each known network destination outside the AS.

■NSSA External (Type 7) – An ASBR within an NSSA generates an NSSA external link state advertisement for each known network destination outside the AS.

### CLI REFERENCES

■"show ip ospf database" on page 1165

### PARAMETERS

These parameters are displayed in the web interface:

- **Process ID** – Process ID as configured in the Network Area configuration screen (see page 506).
- **Query by** – The LSA database can be searched using the following criteria:
  - Self-Originate – LSAs generated by this router.
  - Link ID – LSAs advertising a specific link.
  - Adv Router – LSAs advertised by a specific router.
- **Link State Type** – The information returned by a query can be displayed for all LSA types or for a specific type. (Default: All)

Information displayed for each LSA entry includes:

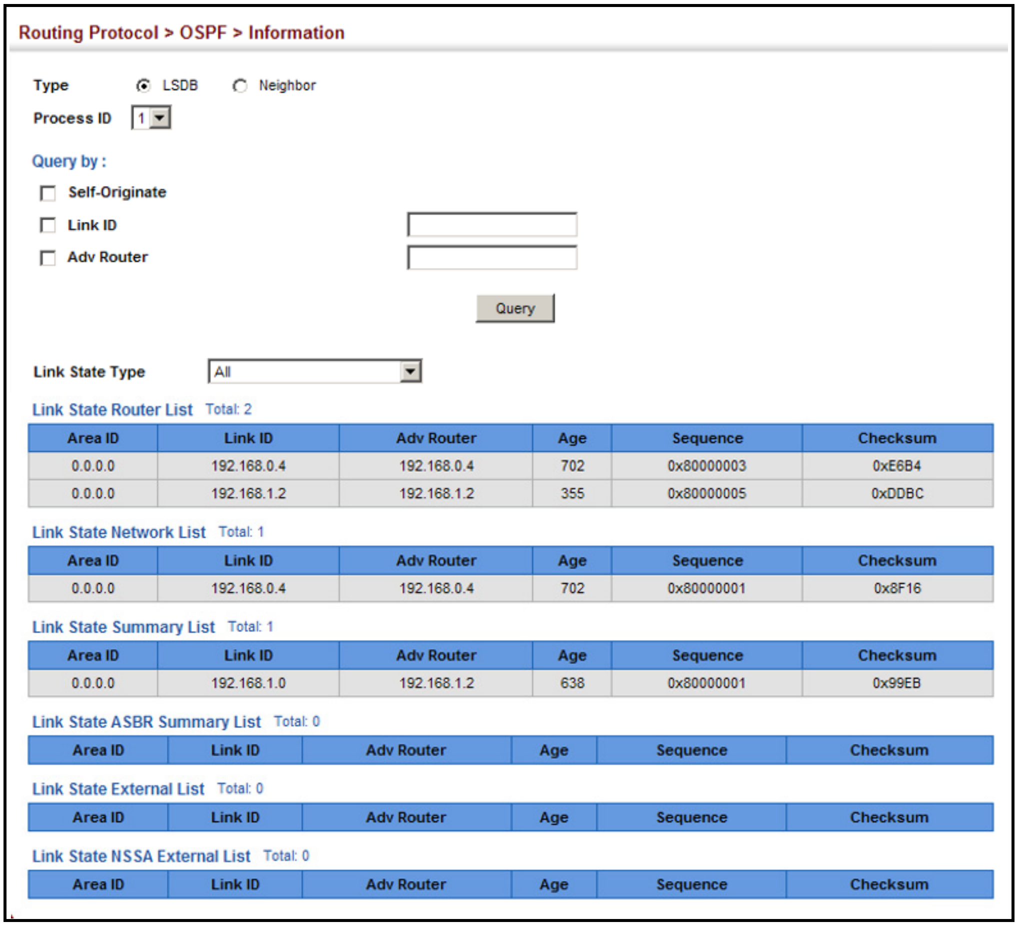
- **Area ID** – Area defined for which LSA information is to be displayed.
- **Link ID** – Network portion described by an LSA. The Link ID is either:
  - An IP network number for Type 3 Summary and Type 5 AS External LSAs. (When an Type 5 AS External LSA is describing a default route, its Link ID is set to the default destination 0.0.0.0.)
  - A Router ID for Router, Network, and Type 4 AS Summary LSAs.
- **Adv Router** – IP address of the advertising router.
- **Age** – Age of LSA (in seconds).
- **Sequence** – Sequence number of LSA (used to detect older duplicate LSAs).
- **Checksum** – Checksum of the complete contents of the LSA.

### WEB INTERFACE

To display information in the link state database:

1. Click Routing Protocol, OSPF, Information.
2. Click LSDB.
3. Select the process identifier.
4. Specify required search criteria, such as self-originated LSAs, LSAs with a specific link ID, or LSAs advertised by a specific router.
5. Then select the database entries to display based on LSA type.

**Figure 51: Displaying Information in the Link State Database**




## DISPLAYING INFORMATION ON NEIGHBORING ROUTERS

Use the Routing Protocol > OSPF > Information (Neighbor) page to display information about neighboring routers on each interface.

### CLI REFERENCES

■ "show ip ospf neighbor" on page 1172

### PARAMETERS

These parameters are displayed in the web interface:

■ **Process ID** – Process ID as configured in the Network Area configuration screen (see page 506).

■ **ID** – Neighbor's router ID.

■ **Priority** – Neighbor's router priority.

■ **State** – OSPF state and identification flag.

States include:

◆ Down – Connection down

- Attempt – Connection down, but attempting contact (non-broadcast networks)
- Init – Have received Hello packet, but communications not yet established
- Two-way – Bidirectional communications established
- ExStart – Initializing adjacency between neighbors
- Exchange – Database descriptions being exchanged
- Loading – LSA databases being exchanged
- Full – Neighboring routers now fully adjacent

Identification flags include:

- D – Dynamic neighbor
- S – Static neighbor
- DR – Designated router
- BDR – Backup designated router

■**Address** – IP address of this interface.

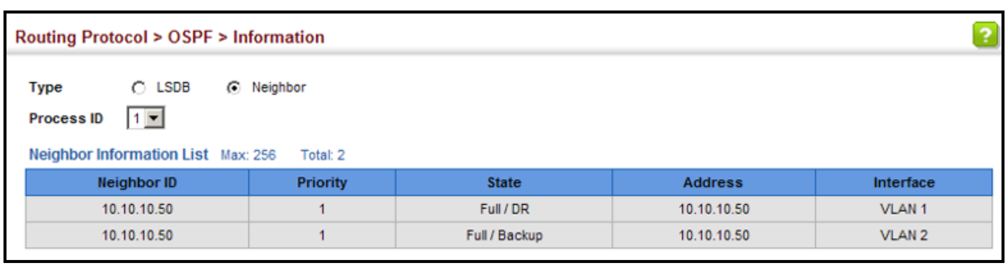
■**Interface** – A Layer 3 interface on which OSPF has been enabled.

### WEB INTERFACE

To display information about neighboring routers stored in the link state database:

1. Click Routing Protocol, OSPF, Information.
2. Click Neighbor.
3. Select the process identifier.

**Figure 52: Displaying Neighbor Routers Stored in the Link State Database**




| Neighbor ID | Priority | State | Address | Interface |
|---|---|---|---|---|
| 10.10.10.50 | 1 | Full / DR | 10.10.10.50 | VLAN 1 |
| 10.10.10.50 | 1 | Full / Backup | 10.10.10.50 | VLAN 2 |

## CONFIGURING THE OPEN SHORTEST PATH FIRST PROTOCOL (VERSION 3)

OSPFv3 supports routing for IPv6, using the same basic mechanisms described in the preceding section for OSPFv2. However, note that OSPFv3 is not backward compatible with OSPFv2. Therefore, if you need to route both IPv4 and IPv6 packets, you will have to run both OSPFv2 and OSPFv3.

Some of the fundamental changes in OSPFv3 include the following items:

- *Per-link protocol processing* – Routing information is passed across the link-local interface with a hop limit of one. Since an IPv6 local link can support multiple global-level subnets, an interface connecting different routers within the same or within different global-level IP subnets can pass protocol-related information. In other words, OSPFv3 runs per-link instead of per-IP-subnet as in OSPFv2.

- *Handling multiple protocol processes* – Where different routing processes run across the same link-local network, an instance identifier is used to indicate a specific process. This identifier has been added to the area and interface configuration commands for this switch.

- *Removal of addressing semantics* – Addressing semantics have been removed from OSPF packets and the basic LSA types. IPv6 addresses are not present in OSPF packet headers. They are only carried in LSA payloads of Link State Update Packets.

- *Removal of IP addressing symantics* – Router LSAs and Network LSAs do not contain IPv6 addresses, but simply express topology information. OSPF Router IDs, Area IDs and LSA Link State IDs remain at the IPv4 size of 32-bits. They cannot be assigned as IPv6 addresses.

- *Consistent Router ID designation* – Neighboring routers are all identified by the Router ID. This removes the inconsistency that existed in OSPFv2, where neighbors were identified by their IP addresses on broadcast and NBMA networks and by their Router IDs on other types of networks.

- *New flooding scope* – Flooding scope for LSAs is now explicitly coded in the LS type field. The area and autonomous system (AS) have been retained from OSPFv2, but now also includes a link-local scope. Flooding for ahe new Link-LSA is restricted to link-local scope, and no further.

- *Use of link-local addresses* – OSPFv3 assumes that each interface has been assigned a link-local unicast address. On all OSPF interfaces except for virtual links, OSPF packets are sent using the interface's link-local unicast address as the source address. A router learns the link-local addresses of all its neighbors, and uses these addresses as their next hop during packet forwarding. On virtual links, global scope or site-local IP addresses must be used as the source for OSPF protocol packets.

- *Authentication removed from protocol packets* – Authentication has been removed from OSPFv3. The authentication extension header provided in IPv6 is used to support required authentication procedures.

- *LSA format changes* – Type 3 (Summary Link) LSAs have been changed to Inter-Area-Prefix LSAs, and Type 4 (AS Summary Link) LSAs have been changed to Inter-Area Router LSAs.

- *New LSA formats* – Two new LSAs have been added, including Type 8 Link LSAs, which carry IPv6 addresses for local links, and Type 9 Intra-Area-Prefix LSAs, which carry IPv6 prefixes for router and network links.

- *Handling unknown LSA types* – Handling of unknown LSA types has been made more flexible so that, based on LS type, unknown LSA types are either treated as having link-local flooding scope, or are stored and flooded as if they were understood. Discarding unknown types causes problems when the Designated Router supports fewer options than the other routers on the link.

*General Configuration Guidelines*

Follow these basic steps to configure OSPFv3:

1. Assign an IPv6 link-local address to each VLAN interface that will participate in an OSPF routing process. You can automatically generate a link-local address using the “Enable IPv6 Explicitly” option on the IP > IPv6 (Configure Interface) page (described on page 421), or manually assign a link-local address to an interface using on the IP > IPv6 (Add IPv6 Address) page (described page 424).

2. Use the Routing Protocol > OSPFv3 > General (Add) page to create a local OSPF router process (see page 539).

3. Use the Routing Protocol > OSPFv3 > Tag (Configure) page to set the Router ID associated with the local OSPF process (see page 540). Note that the default router ID of “0.0.0.0” cannot be used with the current software version.

4. Use the Routing Protocol > OSPFv3 > Interface (Add Area) page to assign an area to each interface that will participate in the specified OSPF process (see page 553).

## CREATING A ROUTING PROCESS

Use the Routing Protocol > OSPFv3 > General (Add) page create an Open Shortest Path First (OSPFv3) routing process.

### CLI REFERENCES

- "router ipv6 ospf" on page 1177

### PARAMETERS

These parameters are displayed in the web interface:

- **Tag Name** – A process name must be entered for each routing process. (Range: Alphanumeric string up to 16 characters)

  The process name is only used on the local router to distinguish between different routing processes. It should not be confused with the Instance ID which is used to distinguish between different routing processes running on the same link-local network segment (see "Configuring OSPFv3 Interfaces" on page 553).

### WEB INTERFACE

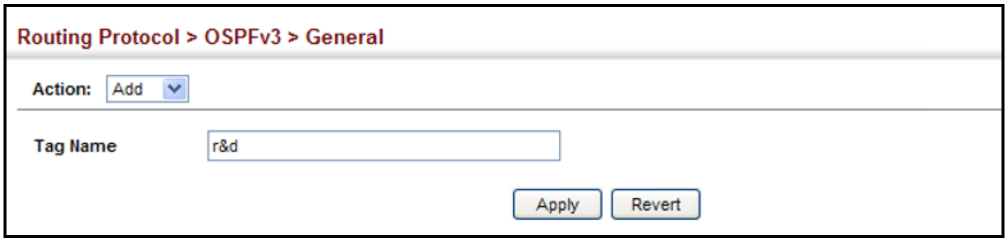
To create an OSPFv3 routing process:

1. Click Routing Protocol, OSPFv3, General.

2. Select Add from the Action list.

3. Enter a name for the routing process.

**Figure 53: Creating a Routing Process**




To show the OSPFv3 routing processes created on the router:

1. Click Routing Protocol, OSPFv3, General.
2. Select Show from the Action list.

**Figure 54: Showing Configured Routing Processes**


## CONFIGURING GENERAL PROTOCOL SETTINGS

To implement OSPFv3 routing, first create a routing process (as described in the preceding section), then use the Routing Protocol > OSPFv3 > Tag (Configure) page to set the basic protocol parameters which will apply to all OSPFv3 interfaces and areas.

### CLI REFERENCES

- "Open Shortest Path First (OSPFv3)" on page 1175

### COMMAND USAGE

- The Redistribute parameter is used to import routes learned from other routing protocols into the OSPF domain, and to generate AS-external-LSAs. When you redistribute external routes into an OSPF autonomous system (AS), the router automatically becomes an autonomous system boundary router (ASBR).

### PARAMETERS

These parameters are displayed in the web interface:

- **Tag Name** – A process name as configured on the Routing Protocol > OSPFv3 > General (Add) page.
- **ABR Type** – Sets the criteria used to determine if this router can declare itself an ABR and issue Type 3 and Type 4 summary LSAs.
  - **Cisco** - ABR criteria and functional behavior is based on RFC 3509. (This is the default setting.)

- **IBM** - ABR criteria and functional behavior is breifly described in RFC 3509, and fully documented in IBM Nways Multiprotocol Routing Services (MRS) 3.3.
- **Standard** - ABR criteria and functional behavior is based on RFC 2328.

The basic criteria for a router to serve as an ABR is shown below:

- Cisco Systems Interpretation: A router is considered to be an ABR if it has more than one area actively attached and one of them is the backbone area.
- IBM Interpretation: A router is considered to be an ABR if it has more than one actively attached area and the backbone area is configured.
- Standard Interpretation: A router is considered to be an ABR if it is attached to two or more areas. It does not have to be attached to the backbone area.

To successfully route traffic to inter-area and AS external destinations, an ABR must be connected to the backbone. If an ABR has no backbone connection, all traffic destined for areas not connected to it or outside the AS will be dropped. This situation is normally resolved, by configuring a virtual link from the ABR to the backbone area.

In both the Cisco and IBM interpretation, a router connected to more than one area cannot issue a Type 1 router LSA declaring itself as an ABR unless it meets the other criteria listed above.

Routing table calculations are changed to allow the router to consider summary-LSAs from all attached areas if it is not an ABR, but has more than one attached area, or it does not have an active backbone connection.

In other words, inter-area routes are calculated by examining summary-LSAs. If the router is an ABR and has an active backbone connection, only backbone summary-LSAs are examined. Otherwise (when either the router is not an ABR or it has no active backbone connection), the router should consider summary-LSAs from all actively attached areas.

This ensures that the summary-LSAs originated by area border routers advertise only intra-area routes into the backbone if the router has an active backbone connection, and advertises both intra-area and inter-area routes into the other areas. Otherwise, the router only advertises intra-area routes into non-backbone areas.

- **Default Metric** – The default metric used for external routes imported from other protocols. (Range: 0-16777214)

  The default metric must be used to resolve the problem of redistributing external routes from other protocols that use incompatible metrics.

  This parameter does not override the metric value set for the Redistribute parameters described below. When a metric value has not been configured for the Redistribute parameters, this parameter sets the metric value to be used for all imported external routes.

- **Max Concurrent DD** – The maximum number of neighbors with which the switch can concurrently exchange database descriptor packets. (Range: 1-65535; Default: 5)

This limit applies separately to the number of neighbors to which DD packets can be concurrently sent, and to the number of neighbors from which DD packets can be concurrently received.

- **Connected Redistribute** – Imports all currently connected entries.
- **Static Redistribute** – Imports IPv6 static routes into this Autonomous System.
- **RIPng Redistribute** – Imports entries learned through the Routing Information Protocol - Nex Generation.
- **Redistribute Metric Type** – The way to advertise routes to destinations outside the AS through External LSAs. (Options: 1, 2)

  When a Type 1 LSA is received by a router, it adds the internal cost to the external route metric. In other words, the cost of the route from any router within the AS is equal to the cost associated with reaching the advertising ASBR, plus the cost of the external route. When a Type 2 LSA is received by a router, it only uses the external route metric to determine route cost.
- **Redistribute Metric** – The metric assigned to all external routes for the specified protocol. (Range: 0-16777214: Default: 10)
- **Router ID** – A unique router ID used for this device within the autonomous system for the current routing process. The Router ID must be formatted as an IPv4 address. (Note that the router ID can also be set to 0.0.0.0 or 255.255.255.255)

  The router ID must be unique for every router in the autonomous system. ~~Using the default setting based on the highest interface address ensures that each router ID is unique.~~

  If this router already has registered neighbors, the new router ID will be used when the router is rebooted, or manually restarted by entering the no router ipv6 ospf followed by the router ipv6 ospf command.

  If the priority values of the routers bidding to be the designated router or backup designated router for an area are equal, the router with the highest ID is elected.

  The current routing process specified by the Tag Name parameter will not be enabled until a Router ID is configured.
- **Delay SFP Timer** – The delay after receiving a topology change notification and starting the SPF calculation. (Range: 0-2147483647 seconds)
- **Hold SFP Timer** – The minimum time between two consecutive SPF calculations. (Range: 0-2147483647 seconds)

  Setting the SPF holdtime to 0 means that there is no delay between consecutive calculations.

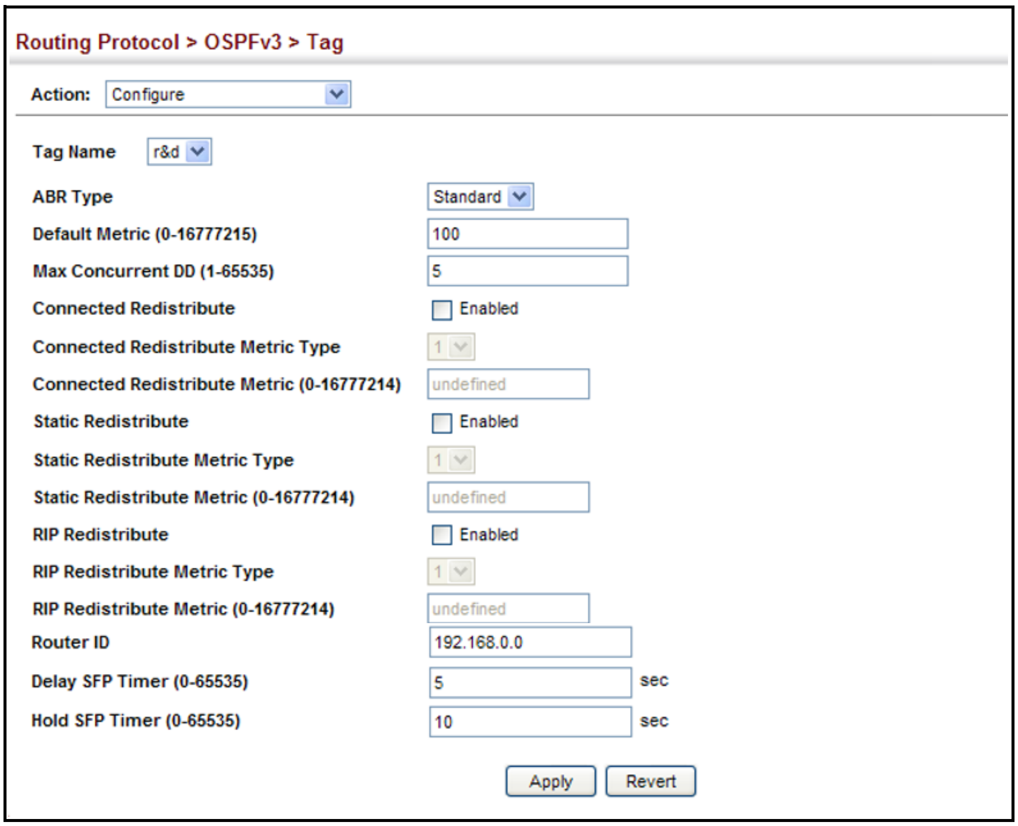
  Using a low value allows the router to switch to a new path faster, but uses more CPU processing time.

### WEB INTERFACE

To configure general protocol settings for OSPF:

1. Click Routing Protocol, OSPFv3, Tag.
2. Select Configure from the Action list.
3. Select a Tag name, and then specify the Router ID and other global attributes as required.
4. Click Apply

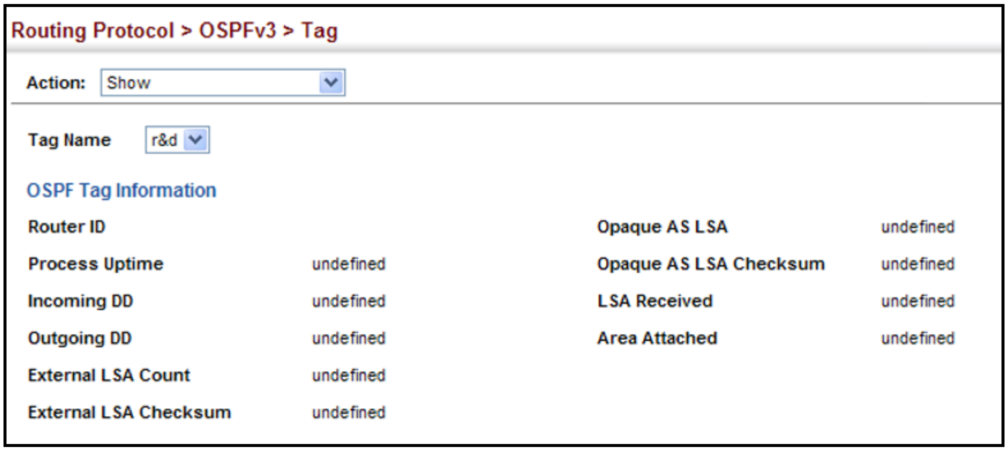
**Figure 55: Configure General Settings for OSPFv3**




To show adminstrative settings and statistics for OSPF:

1. Click Routing Protocol, OSPFv3, Tag.
2. Select Show from the Action list.

**Figure 56: Showing General Settings for OSPFv3**




## SETTING AN INTERFACE TO PASSIVE MODE

Use the Routing Protocol > OSPFv3 > Tag (Configure Passive Interface) page to suppress OSPF routing traffic on the specified interface.

### CLI REFERENCES

- "passive-interface" on page 1194

### COMMAND USAGE

- You can configure an OSPF interface as passive to prevent OSPF routing traffic from exiting or entering that interface. No OSPF adjacency can be formed if one of the interfaces involved is set to passive mode. The specified interface will appear as a stub in the OSPF domain. Also, if you configure an OSPF interface as passive where an adjacency already exists, the adjacency will drop almost immediately.

### PARAMETERS

These parameters are displayed in the web interface:

- **Tag Name** – A process name as configured on the Routing Protocol > OSPFv3 > General (Add) page.

- **VLAN** – VLAN ID. (Range: 1-4093)

- **Status** – Enables or disables routing traffic on the specified interface.

### WEB INTERFACE

To set an interface to passive mode:

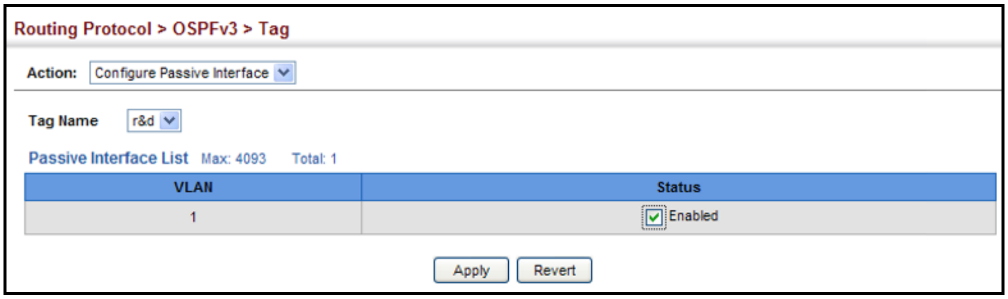
1. Click Routing Protocol, OSPFv3, Tag.

2. Select Configure Passive Interface from the Action list.

3. Select a Tag name, and then enable passive routing mode on the required interface.

4. Click Apply

**Figure 57: Setting an Interface to Passive Mode**




## ADDING A STUB

Use the Routing Protocol > OSPF > Area (Configure Area – Add Area) page to add a stubby area (Stub).

### CLI REFERENCES

- "router ipv6 ospf" on page 1177
- "area stub" on page 1185

### COMMAIND USAGE

- This router supports up to 256 stubs.

### PARAMETERS

These parameters are displayed in the web interface:

- **Tag Name** – A process name as configured on the Routing Protocol > OSPFv3 > General (Add) page.
- **Area ID** – Identifies the stub area. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

  All routers in a stub must be configured with the same area ID.
- **Default Cost** – Cost for the default summary route sent into a stub from an area border router (ABR). (Range: 0-16777215; Default: 0)

  Note that whe the default cost is set to “0,” the router will not advertise a default route into the attached stub.
- **Summary** – Controls the use of summary routes.
  - **Summary** – Allows an Area Border Router (ABR) to send a summary link advertisement into the stub area.

    Routing table space is saved by stopping an ABR from flooding Type-4 Inter-Area Router and Type 5 AS-External LSAs into the stub. Since no information on external routes is known inside the stub, an ABR will advertise the default route 0::0/0 using a Type 3 Inter-Area Prefix LSA.

    The default setting for a stub blocks Type-4 Inter-Area Router and Type 5 AS-External LSAs. Therefore, any destinations that cannot be matched to an inter-area or intra-area route will have to use the default route.
  - **No Summary** – Stops an ABR from sending a summary link advertisement into a stub area.

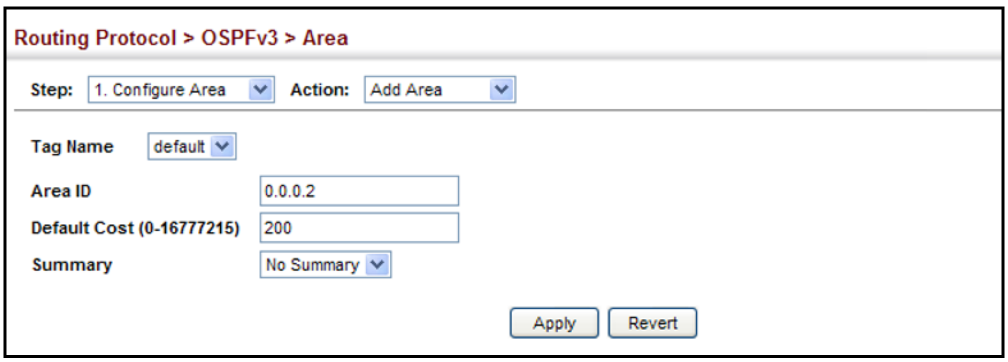
Use this option on an ABR attached to the stub to define a totally stubby area, blocking all Type 3 network summary LSAs. Define an area as a totally stubby area only if routers in the area do not require summary LSAs from other areas.

### WEB INTERFACE

To configure protocol settings for a stub:

1. Click Routing Protocol, OSPFv3, Area.
2. Select Configure Area from the Step list.
3. Select Add Area from the Action list.
4. Select a Tag name, set the cost used for the default summary route sent into the stub, or specify whether or not to make the stub totally stubby by suppressing the summary route.
5. Click Apply

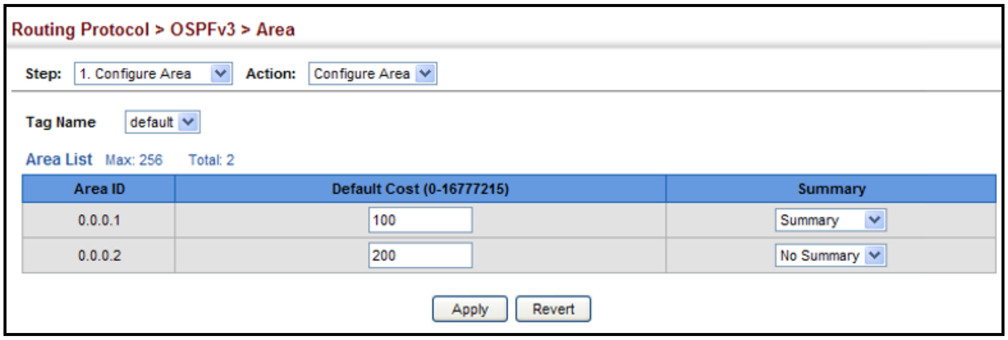
**Figure 58: Adding a Stub**




To configure protocol settings for an existing stub:

1. Click Routing Protocol, OSPFv3, Area.
2. Select Configure Area from the Step list.
3. Select Configure Area from the Action list.
4. Select a Tag name, set the cost used for the default summary route sent into the stub, or specify whether or not to make the stub totally stubby by suppressing the summary route.
5. Click Apply

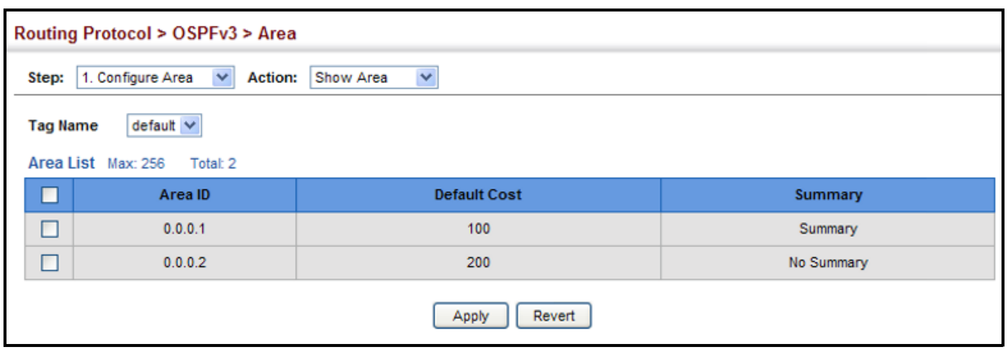
**Figure 59: Configuring an Existing Stub**




To show the protocol settings for all stubs:

1. Click Routing Protocol, OSPFv3, Area.
2. Select Configure Area from the Step list.
3. Select Show Area from the Action list.
4. Select a Tag name.

**Figure 60: Showing All Stubs**




## DISPLAYING INFORMATION ON STUBS

Use the Routing Protocol > OSPF > Area (Show Information) page to display protocol information on stubby areas.

### CLI REFERENCES

- "show ipv6 ospf database" on page 1196

### PARAMETERS

These parameters are displayed in the web interface:

- **Tag Name** – A process name as configured on the Routing Protocol > OSPFv3 > General (Add) page.
- **Link State ID** – This field identifies the piece of the routing domain that is being described by the advertisement.
- **ADV Router** – Advertising router ID.
- **Age** – Age of LSA (in seconds).

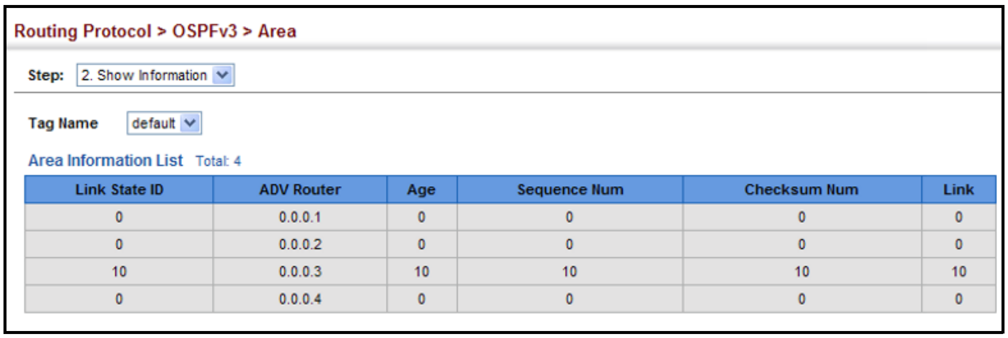
- **Sequence Num** – Sequence number of LSA (used to detect older duplicate LSAs).
- **Checksum ~~Num~~** – Checksum of the complete contents of the LSA.
- **Link** – Number of interfaces attached to the router.

### WEB INTERFACE

To display information on stubs:

1. Click Routing Protocol, OSPFv3, Area.
2. Select Show Information from the Action list.
3. Select a tag name.

**Figure 61: Displaying Information on Stubs**


Routing Protocol > OSPFv3 > Area

Step: 2. Show Information

Tag Name default

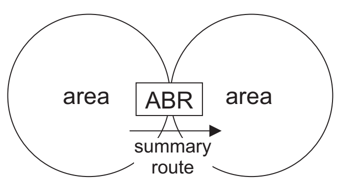
Area Information List Total: 4

| Link State ID | ADV Router | Age | Sequence Num | Checksum Num | Link |
|---|---|---|---|---|---|
| 0 | 0.0.0.1 | 0 | 0 | 0 | 0 |
| 0 | 0.0.0.2 | 0 | 0 | 0 | 0 |
| 10 | 0.0.0.3 | 10 | 10 | 10 | 10 |
| 0 | 0.0.0.4 | 0 | 0 | 0 | 0 |

## CONFIGURING AREA RANGES (ROUTE SUMMARIZATION FOR ABRS)

An OSPF area can include a large number of nodes. If the Area Border Router (ABR) has to advertise route information for each of these nodes, this wastes a lot of bandwidth and processor time. Instead, you can use the Routing Protocol > OSPFv3 > Area Range (Add) page to configure an ABR to advertise a single summary route that covers all the individual networks within its area. When using route summaries, local changes do not have to be propagated to other area routers. This allows OSPF to be easily scaled for larger networks, and provides a more stable network topology.

**Figure 62: Route Summarization for ABRs**




### CLI REFERENCES

- "router ipv6 ospf" on page 1177
- "area range" on page 1182

### COMMAND USAGE

- Use the Area Range configuration page to summarize intra-area routes, and advertise this information to other areas through Area Border Routers (ABRs). The summary route for an area is defined by an IPv6 prefix. You therefore need to structure each area with a contiguous set of addresses so that all routes in the area fall within an easily specified range. If it is not possible to use one contiguous set of addresses, then the routes can be summarized for several area ranges.

- This router supports up 64 summary routes for area ranges.

### PARAMETERS

These parameters are displayed in the web interface:

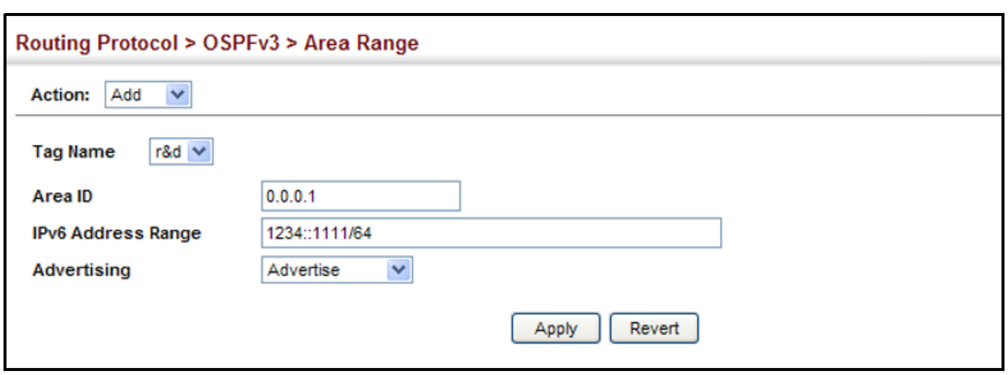
- **Tag Name** – A process name as configured on the Routing Protocol > OSPFv3 > General (Add) page.
- **Area ID** – Identifies an area for which the routes are summarized. The area ID can be in the form of an IPv4 address, or also as a four octet unsigned integer ranging from 0-4294967295.
- **IPv6 Address Range** – A full IPv6 address including the network prefix and host address bits, followed by a forward slash and the prefix length indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the portion of the address to summarize).
- **Advertising** – Indicates whether or not to advertise the summary route. If the routes are set to be advertised, the router will issue a Type 3 network summary LSA for the specified address range. If the summary is not advertised, the specified routes remain hidden from the rest of the network. (Default: Advertise)

### WEB INTERFACE

To configure a route summary for an area range:

1. Click Routing Protocol, OSPFv3, Area Range.
2. Select Add from the Action list.
3. Select a Tag name. Enter an area identifier, the IPv6 address and prefix length for the routes to summarize, and then select whether or not to advertise the summary route to other areas.
4. Click Apply

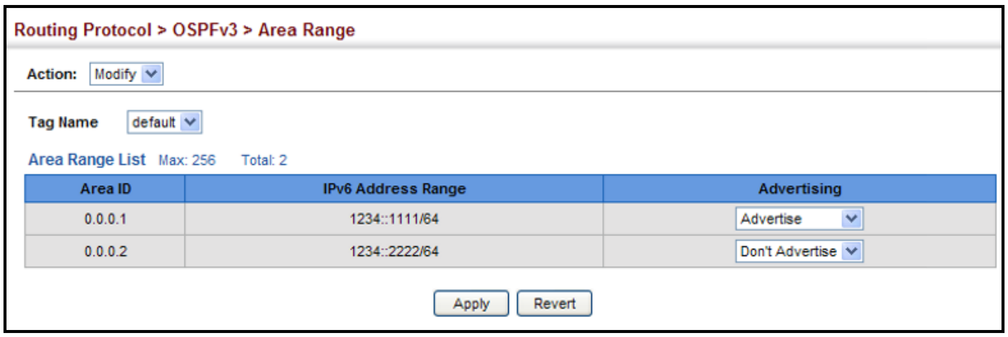
**Figure 63: Configuring Route Summaries for an Area Range**



To modify a route summary for an area range:

1. Click Routing Protocol, OSPFv3, Area Range.
2. Select Modify from the Action list.
3. Select a Tag name, and then select whether or not to advertise the summary route to other areas.
4. Click Apply

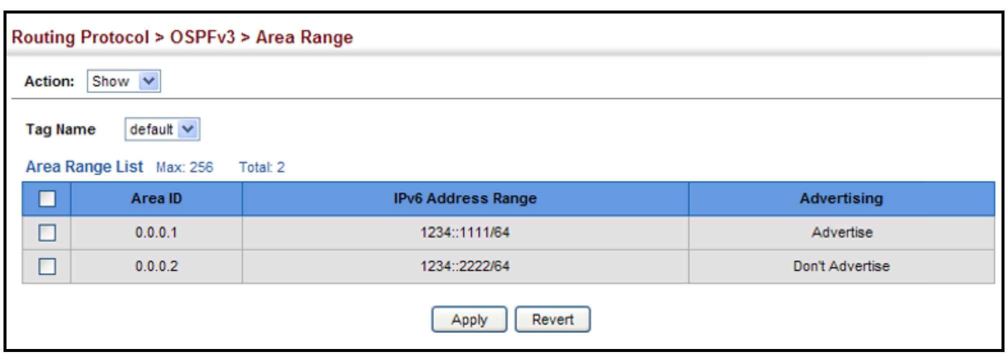
**Figure 64: Modifying Route Summaries for an Area Range**




To show the configured route summaries:

1. Click Routing Protocol, OSPFv3, Area Range.
2. Select Show from the Action list.
3. Select a Tag name.

**Figure 65: Showing Configured Route Summaries**

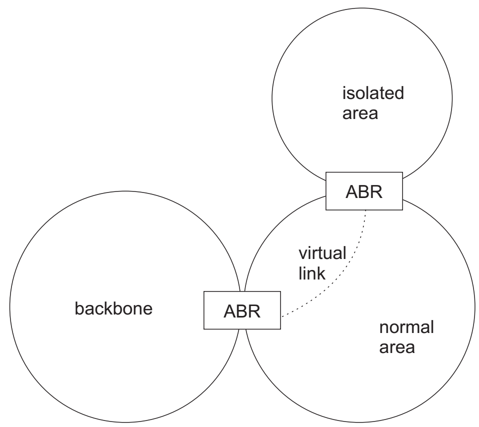



## CONFIGURING VIRTUAL LINKS

Use the Routing Protocol > OSPFv3 > Virtual Link (Add) and (Configure Detailed Settings) pages to configure a virtual link from an area that does not have a direct physical connection to the OSPF backbone.

All OSPF areas must connect to the backbone. If an area does not have a direct physical connection to the backbone, you can configure a virtual link that provides a logical path to the backbone. To connect an isolated area to the backbone, the logical path can cross a single non-backbone area (i.e., transit area) to reach the backbone. To define this path, you must configure an ABR that serves as an endpoint connecting the isolated area to the common transit area, and specify a neighboring ABR at the other endpoint connecting the common transit area to the backbone itself. (Note that you cannot configure a virtual link that runs through a stub ~~or NSSA~~.)

**Figure 66: OSPF Virtual Link**




Virtual links can also be used to create a redundant link between any area and the backbone to help prevent partitioning, or to connect two existing backbone areas into a common backbone.

Any area disconnected from the backbone must include the transit area ID and the router ID for a virtual link neighbor that is adjacent to the backbone.

This router supports up five virtual links.

### CLI REFERENCES

- "router ipv6 ospf" on page 1177
- "area virtual-link" on page 1186

### COMMAND USAGE

- Use the Add page to create a virtual link, and then use the Configure Detailed Settings page to set the protocol timers for the link. The parameters to configure on the Configure Detailed Settings page are described under "Configuring OSPFv3 Interfaces" on page 553.

### PARAMETERS

These parameters are displayed in the web interface:

- **Tag Name** – A process name as configured on the Routing Protocol > OSPFv3 > General (Add) page.

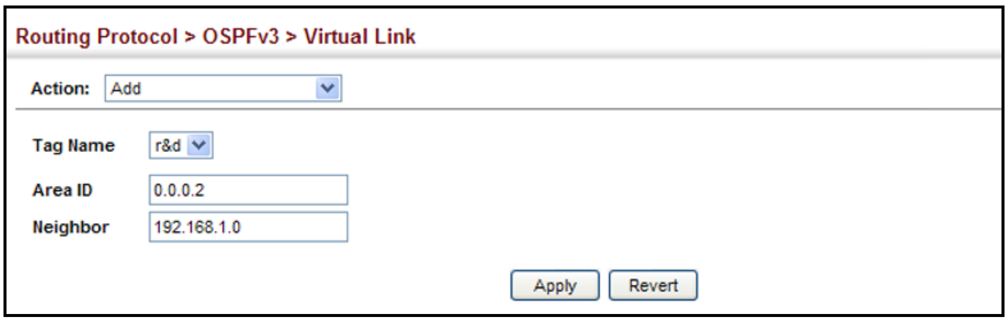
- **Area ID** – Identifies the transit area for the virtual link. The area ID can be in the form of an IPv4 address, or as a four octet unsigned integer ranging from 0-4294967295.

- **Neighbor** – Web Interface

To create a virtual link:

1. Click Routing Protocol, OSPFv3, Virtual Link.
2. Select Add from the Action list.
3. Specify the Tag Name, the Area ID, and Neighbor router ID.
4. Click Apply.

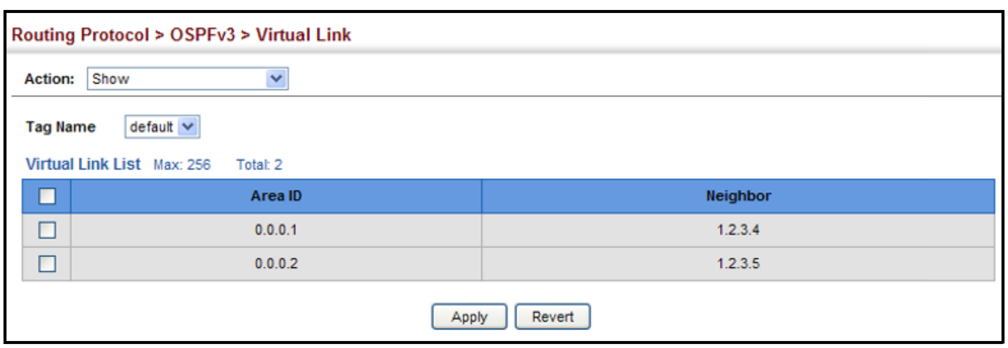
**Figure 67: Adding a Virtual Link**




To show virtual links:

1. Click Routing Protocol, OSPFv3, Virtual Link.
2. Select Show from the Action list.
3. Select the Tag name.

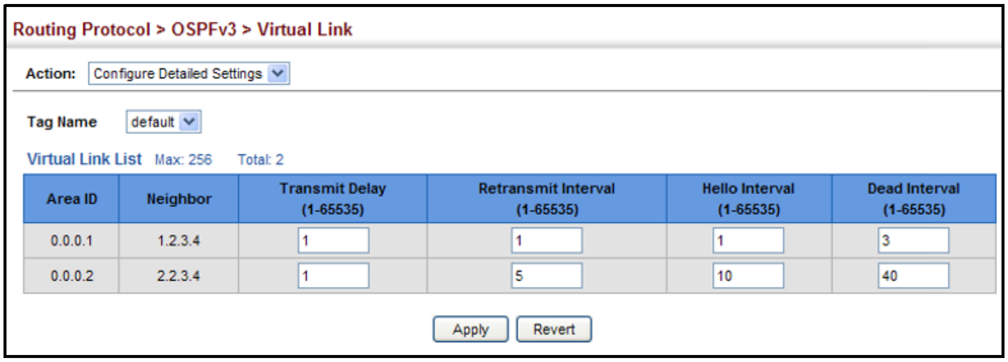
**Figure 68: Showing Virtual Links**




To configure detailed settings for a virtual link:

1. Click Routing Protocol, OSPFv3, Virtual Link.
2. Select Configure Detailed Settings from the Action list.
3. Specify the tag name, and then modify the protocol timers as required.
4. Click Apply.

**Figure 69: Configuring Detailed Settings for a Virtual Link**




## CONFIGURING OSPFV3 INTERFACES

You should specify a routing interface for any local subnet that needs to communicate with other network segments located on this router or elsewhere in the network. First configure a VLAN for each subnet that will be directly connected to this router, and assign IPv6 interfaces to each of these VLANs. Then create an OSPFv3 process, and assign a router ID to this device. (See the General Configuration Guidelines at the beginning of OSPFv3 section.)

Use the Routing Protocol > OSPFv3 > Interface (Add Area) page to bind an OSPF area to a Layer 3 interface. Then use the (Configure) page to configure the interface-specific parameters used by OSPF to select the designated router, set the cost used to select preferred paths, control the timing of link state advertisements.

### CLI REFERENCES

- "Open Shortest Path First (OSPFv3)" on page 1175

### PARAMETERS

These parameters are displayed in the web interface:

*Add Area*

- **VLAN ID** – A VLAN to which an IPv6 interface has been assigned.

- **Instance ID** – Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface. (Range: 0-255)

- **Area ID** – Area to bind to the current Layer 3 interface. An OSPF area identifies a group of routers that share common routing information. The area ID can be in the form of an IPv4 address, or as a four octet unsigned integer ranging from 0-4294967295.

- **Tag Name** – A process name as configured on the Routing Protocol > OSPFv3 > General (Add) page.

*Configure*

- **VLAN ID** – A VLAN to which an IPv6 interface has been assigned.

- **Instance ID** – Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface. (Range: 0-255)

- **Cost** – Sets the cost of sending a protocol packet on an interface, where higher values indicate slower ports. (Range: 1-65535; Default: 1)

  The interface cost indicates the overhead required to send packets across a certain interface. This is advertised as the link cost in router link state advertisements.

  Routes are assigned a metric equal to the sum of all metrics for each interface link in the route.

  This router uses a default cost of 1 for all ports. Therefore, if you install a 10 Gigabit module, you may need to reset the cost for all other VLAN interfaces with only 1 Gbps ports to a value greater than 1 to reflect the actual interface bandwidth.

- **Priority** – Sets the interface priority for this router. (Range: 0-255; Default: 1)

  This priority determines the designated router (DR) and backup designated router (BDR) for each OSPF area. The DR forms an active adjacency to all other routers in the area to exchange routing topology information. If for any reason the DR fails, the BDR takes over this role.

  Set the priority to zero to prevent a router from being elected as a DR or BDR. If set to any value other than zero, the router with the highest priority becomes the DR and the router with the next highest priority becomes the BDR. If two or more routers are set to the same highest priority, the router with the higher ID will be elected.

  If a DR already exists for an area when this interface comes up, the new router will accept the current DR regardless of its own priority. The DR will not change until the next time the election process is initiated.

  Configure router priority for multi-access networks only and not for point-to-point networks.

- **Hello Interval** – Sets the interval between sending hello packets on an interface. This interval must be set to the same value for all routers on the network. (Range: 1-65535 seconds; Default: 10)

  Hello packets are used to inform other routers that the sending router is still active. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase routing traffic.

- **Dead Interval** – Sets the interval at which hello packets are not seen before neighbors declare the router down. This interval must be set to the same value for all routers on the network. (Range: 1-65535 seconds; Default: 40 seconds, or 4 times the Hello Interval)

  The dead-interval is advertised in the router's hello packets. It must be a multiple of hello-interval and be the same for all routers on a specific network.

- **Transmit Delay** – Sets the estimated time to send a link-state update packet over an interface. (Range: 1-65535 seconds; Default: 1 second)

  LSAs have their age incremented by this delay before transmission. You should consider both the transmission and propagation delays for an interface when estimating this delay. Set the transmit delay according to link speed, using larger values for lower-speed links.

If this delay is not added, the time required to transmit an LSA over the link is not taken into consideration by the routing process. On slow links, the router may send packets more quickly than devices can receive them. To avoid this problem, you can use the transmit delay to force the router to wait a specified interval between transmissions.

- **Retransmit Interval** – Sets the time between resending link-state advertisements. (Range: 1-65535 seconds; Default: 5 seconds)

  A router will resend an LSA to a neighbor if it receives no acknowledgment after the specified retransmit interval. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. Note that this value should be larger for virtual links.

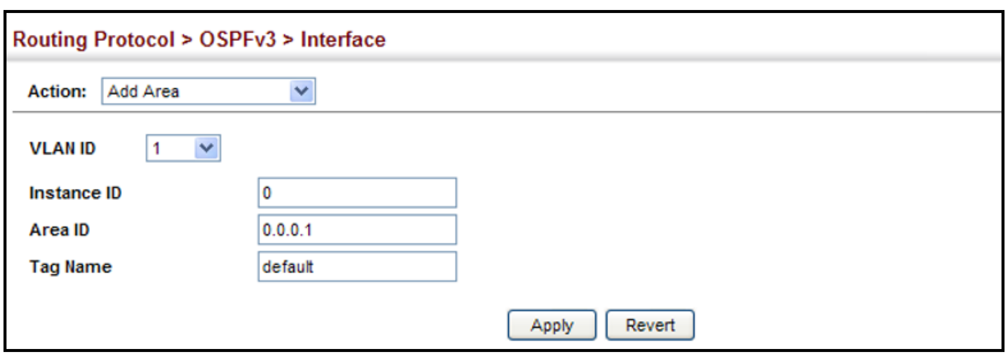
  Set this interval to a value that is greater than the round-trip delay between any two routers on the attached network to avoid unnecessary retransmissions.

### WEB INTERFACE

To bind an OSPF area to a Layer 3 interface:

1. Click Routing Protocol, OSPFv3, Interface.
2. Select Add Area from the Action list.
3. Select the VLAN ID, configure the instance ID if multiple OSPFv3 routing processes are to run over the same interface, set the area ID, and the name of the local process.
4. Click Apply.

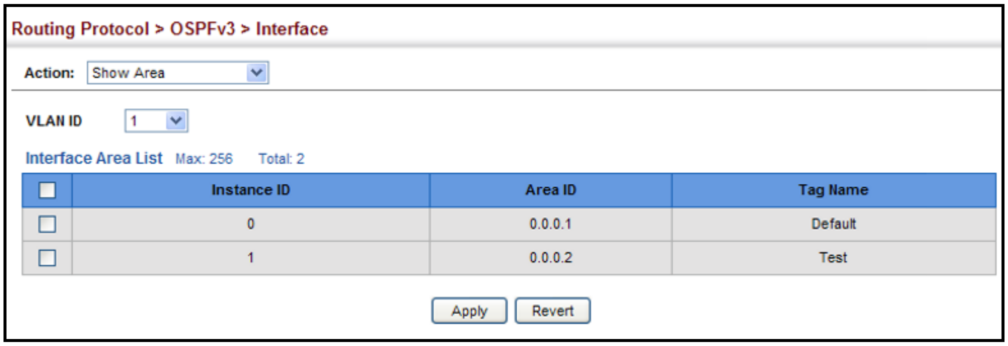
**Figure 70: Binding an OSPFv3 Area to an Interface**




To show the OSPF areas bound to an interface:

1. Click Routing Protocol, OSPFv3, Interface.
2. Select Show from the Action list.
3. Select the VLAN ID.

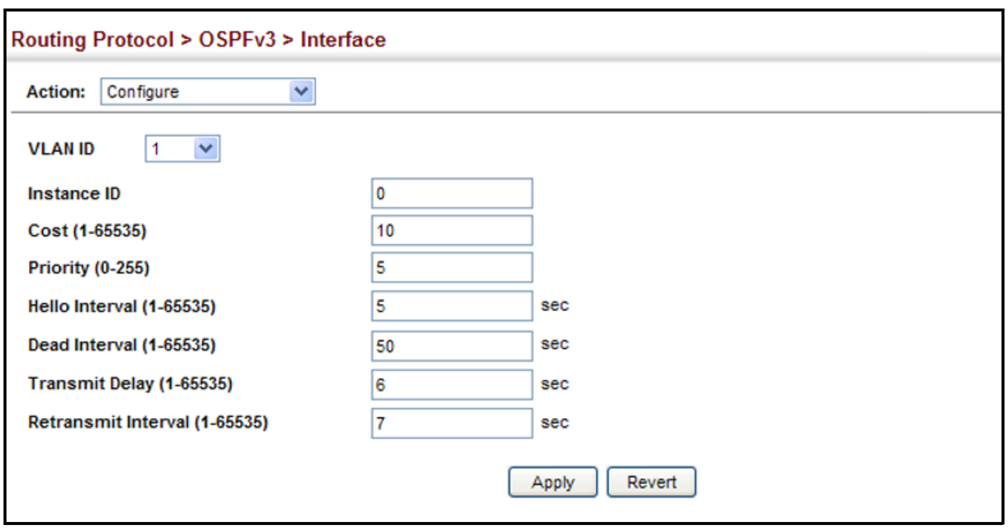
**Figure 71: Showing OSPFv3 Areas Bound to an Interface**




To configure OSPF protocol settings for a Layer 3 interface:

1. Click Routing Protocol, OSPFv3, Interface.
2. Select Configure from the Action list.
3. Select the VLAN ID, and then configure the parameters used by OSPF to select the designated router, select preferred paths, and control the timing of link state advertisements.
4. Click Apply.

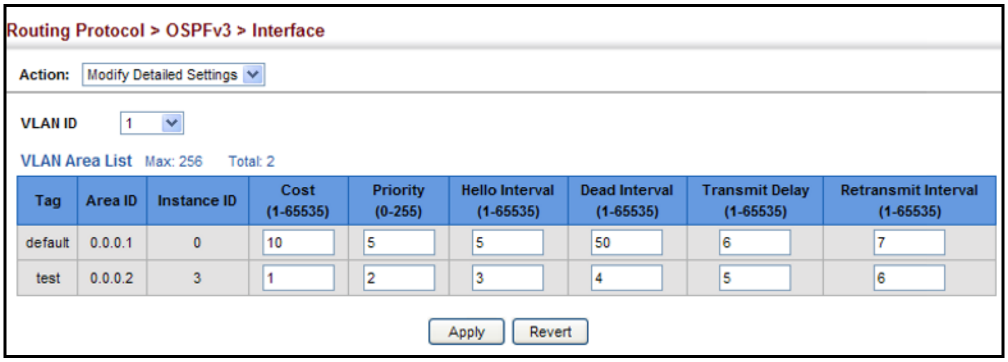
**Figure 72: Configuring OSPFv3 Parameters for an Interface**




To display or modify the OSPF protocol settings for a Layer 3 interface:

1. Click Routing Protocol, OSPFv3, Interface.
2. Select Modify Detailed Settings from the Action list.
3. Select the VLAN ID, and modify the require protocol parameters.
4. Click Apply.

**Figure 73: Displaying or Modifying OSPFv3 Parameters for an Interface**



Routing Protocol > OSPFv3 > Interface

Action: Modify Detailed Settings

VLAN ID 1

VLAN Area List Max: 256 Total: 2

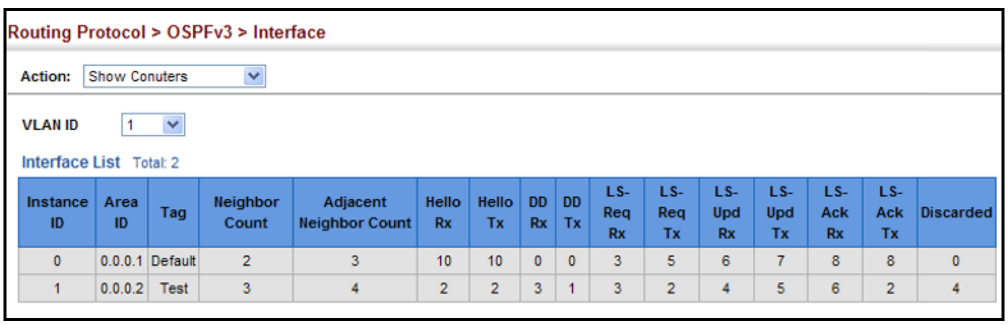
| Tag | Area ID | Instance ID | Cost (1-65535) | Priority (0-255) | Hello Interval (1-65535) | Dead Interval (1-65535) | Transmit Delay (1-65535) | Retransmit Interval (1-65535) |
|---|---|---|---|---|---|---|---|---|
| default | 0.0.0.1 | 0 | 10 | 5 | 5 | 50 | 6 | 7 |
| test | 0.0.0.2 | 3 | 1 | 2 | 3 | 4 | 5 | 6 |

Apply Revert

To show information on neighboring routers and the exchange of protocol messages for OSPFv3 interfaces:

1. Click Routing Protocol, OSPF, Interface.
2. Select Show Counters from the Action list.
3. Select the VLAN ID. (For a description of the information displayed see page 1197.)

**Figure 74: Showing Protocol Counters OSPFv3 Interfaces**



Routing Protocol > OSPFv3 > Interface

Action: Show Conuters

VLAN ID 1

Interface List Total: 2

| Instance ID | Area ID | Tag | Neighbor Count | Adjacent Neighbor Count | Hello Rx | Hello Tx | DD Rx | DD Tx | LS-Req Rx | LS-Req Tx | LS-Upd Rx | LS-Upd Tx | LS-Ack Rx | LS-Ack Tx | Discarded |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0.0.0.1 | Default | 2 | 3 | 10 | 10 | 0 | 0 | 3 | 5 | 6 | 7 | 8 | 8 | 0 |
| 1 | 0.0.0.2 | Test | 3 | 4 | 2 | 2 | 3 | 1 | 3 | 2 | 4 | 5 | 6 | 2 | 4 |

## SHOWING OSPFV3 INTERFACE STATUS

Use the Routing Protocol > OSPFv3 > Interface (Show) page to show the status of OSPFv3 interfaces.

### CLI REFERENCES

- "show ipv6 ospf interface" on page 1197

### PARAMETERS

These parameters are displayed in the web interface:

- **Status** – The status of physical link (i.e., up or down).
- **Link Local IP** – Link local address of OSPF interface.
- **Area ID** – OSPF area to which this interface belongs.
- **Tag** – OSPF process identifier string.

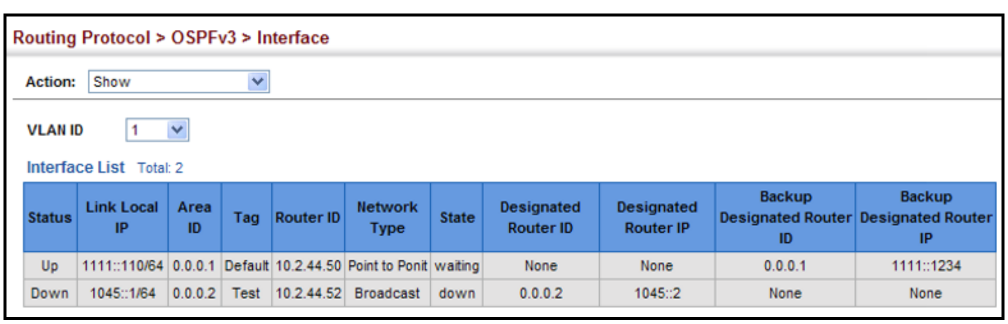
- **Router ID** – Identifier for this router.
- **Network Type** – Includes broadcast, non-broadcast, or point-to-point networks.
- **State** – Interface status:
  - Disabled – OSPF not enabled on this interface
  - Down – OSPF is enabled on this interface, but interface is down
  - Loopback – This is a loopback interface
  - Waiting – Router is trying to find the DR and BDR
  - DR – Designated Router
  - BDR – Backup Designated Router
  - DROther – Interface is on a multiaccess network, but is not the DR or BDR
- **Designated Router ID** – Identifier of the designated router for the area to which this router is attached.
- **Designated Router IP** – Interface address of the designated router for the area to which this router is attached.
- **Backup Designated Router ID** – Identifier of the backup designated router for the area to which this router is attached.
- **Backup Designated Router IP** – Interface address of the backup designated router for the area to which this router is attached.

## WEB INTERFACE

To show the status of OSPFv3 interfaces: (Steve> Many of the preceeding web pages all have problems. Functions can be configured and displayed in the cli, but not in the web. Stopping reveiw at this point.)

1. Click Routing Protocol, OSPF, Interface.
2. Select Show from the Action list.
3. Select the VLAN ID. (For a description of the information displayed see page 1197.)

**Figure 75: Showing the Status of OSPFv3 Interfaces**




| Status | Link Local IP | Area ID | Tag | Router ID | Network Type | State | Designated Router ID | Designated Router IP | Backup Designated Router ID | Backup Designated Router IP |
|---|---|---|---|---|---|---|---|---|---|---|
| Up | 1111::110/64 | 0.0.0.1 | Default | 10.2.44.50 | Point to Ponit | waiting | None | None | 0.0.0.1 | 1111::1234 |
| Down | 1045::1/64 | 0.0.0.2 | Test | 10.2.44.52 | Broadcast | down | 0.0.0.2 | 1045::2 | None | None |

## SHOWING OSPFV3 INTERFACE PROTOCOL COUNTERS

Use the Routing Protocol > OSPFv3 > Interface (Show Counters) page to show information on neighboring routers and the exchange of protocol messages for OSPFv3 interfaces:

### CLI REFERENCES

■"show ipv6 ospf interface" on page 1197

### PARAMETERS

These parameters are displayed in the web interface:

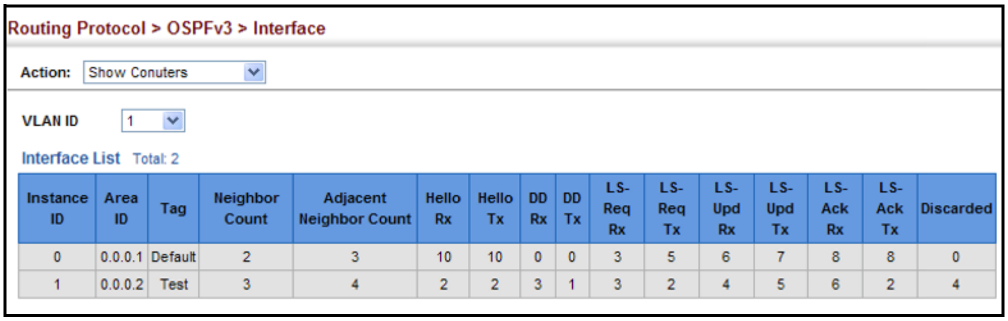
- **Instance ID** – Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface.
- **Area ID** – OSPF area to which this interface belongs.
- **Tag** – OSPF process identifier string.
- **Neighbor Count** – Number of network neighbors.
- **Adjacent Neighbor Count** – Number of adjacent neighbors.
- **Hello Rx** – Number of Hello LSAs received.
- **Hello Tx** – Number of Hello LSAs sent.
- **DD Rx** – Number of Database Descriptor packets received.
- **DD Tx** – Number of Database Descriptor packets sent.
- **LS-Req Rx** – Number of LSA update requests received.
- **LS-Req Tx** – Number of LSA updates requests sent.
- **LS-Upd Rx** – Number of LSA updates received.
- **LS-Upd Tx** – Number of LSA updates sent.
- **LS-Ack Rx** – Number of LSA acknowledgements received.
- **LS-Ack Tx** – Number of LSA acknowledgements sent.
- **Discarded** – Number of LSAs discarded.

### WEB INTERFACE

To display information on neighboring routers and the exchange of protocol messages for OSPFv3 interfaces:

1. Click Routing Protocol, OSPF, Interface.
2. Select Show Counters from the Action list.
3. Select the VLAN ID.

**Figure 76: Showing Protocol Counters OSPFv3 Interfaces**




| Instance ID | Area ID | Tag | Neighbor Count | Adjacent Neighbor Count | Hello Rx | Hello Tx | DD Rx | DD Tx | LS-Req Rx | LS-Req Tx | LS-Upd Rx | LS-Upd Tx | LS-Ack Rx | LS-Ack Tx | Discarded |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0.0.0.1 | Default | 2 | 3 | 10 | 10 | 0 | 0 | 3 | 5 | 6 | 7 | 8 | 8 | 0 |
| 1 | 0.0.0.2 | Test | 3 | 4 | 2 | 2 | 3 | 1 | 3 | 2 | 4 | 5 | 6 | 2 | 4 |

## DISPLAYING INFORMATION ON NEIGHBORING ROUTERS

Use the Routing Protocol > OSPFv3 > Information (Neighbor) page to display information about neighboring routers on each interface.

### CLI REFERENCES

■"show ipv6 ospf neighbor" on page 1198

### PARAMETERS

These parameters are displayed in the web interface:

■**Tag Name** – A process name as configured on the Routing Protocol > OSPFv3 > General (Add) page.

■**ID** – Neighbor's router ID.

■**Priority** – Neighbor's router priority.

■**State** – OSPF state and identification flag.

States include:

- Down – Connection down
- Attempt – Connection down, but attempting contact (non-broadcast networks)
- Init – Have received Hello packet, but communications not yet established
- Two-way – Bidirectional communications established
- ExStart – Initializing adjacency between neighbors
- Exchange – Database descriptions being exchanged
- Loading – LSA databases being exchanged
- Full – Neighboring routers now fully adjacent

Identification flags include:

- D – Dynamic neighbor
- S – Static neighbor
- DR – Designated router
- Backup – Backup designated router

■ **Interface ID** – Index for this interface.

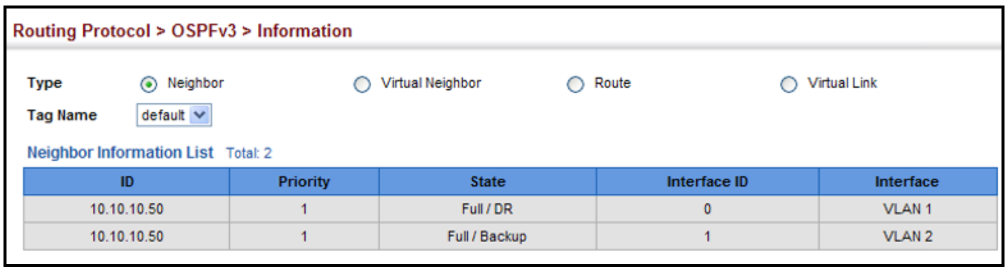
■ **Interface** – A Layer 3 interface on which OSPF has been enabled.

### WEB INTERFACE

To display information about neighboring routers stored in the link state database:

1. Click Routing Protocol, OSPFv3, Information.
2. Click Neighbor.
3. Select the tag name.

**Figure 77: Displaying Neighbor Routers Stored in the Link State Database**




## DISPLAYING INFORMATION ON VIRTUAL NEIGHBORS

Use the Routing Protocol > OSPFv3 > Information (Virtual Neighbor) page to show information about the neighbor router assigned to the other end of a virtual link (see "Configuring Virtual Links" on page 550).

### CLI REFERENCES

■ "show ip ospf virtual-links" on page 1174

### PARAMETERS

These parameters are displayed in the web interface:

■ **Tag Name** – A process name as configured on the Routing Protocol > OSPFv3 > General (Add) page.

■ **ID** – Neighbor's router ID.

■ **Priority** – Neighbor's router priority.

■ **State** – The adjancy state of the virtual neighbor relationship:

- Down – Connection down
- Attempt – Connection down, but attempting contact (non-broadcast networks)
- Init – Have received Hello packet, but communications not yet established
- Two-way – Bidirectional communications established
- ExStart – Initializing adjacency between neighbors
- Exchange – Database descriptions being exchanged

- Loading – LSA databases being exchanged
- Full – Neighboring routers now fully adjacent

■**Interface ID** – Index for this interface.

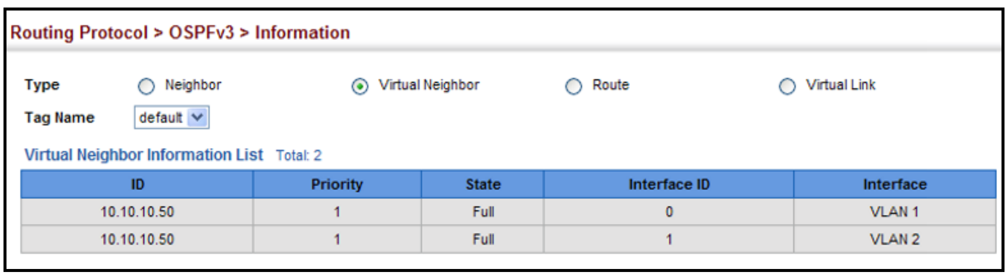
■**Interface** – Interface through which the virtual neighbor can be reached.

### WEB INTERFACE

To display information about virtual neighbors:

1. Click Routing Protocol, OSPFv3, Information.
2. Click Virtual Neighbor.
3. Select the tag name.

**Figure 78: Displaying Information on Virtual Neighbors**




| ID | Priority | State | Interface ID | Interface |
|---|---|---|---|---|
| 10.10.10.50 | 1 | Full | 0 | VLAN 1 |
| 10.10.10.50 | 1 | Full | 1 | VLAN 2 |

## DISPLAYING THE OSPFV3 ROUTING TABLE

Use the Routing Protocol > OSPFv3 > Information (Route) page to show the OSPF routing table.

### CLI REFERENCES

■"show ipv6 ospf route" on page 1199

### PARAMETERS

These parameters are displayed in the web interface:

■**Tag Name** – A process name as configured on the Routing Protocol > OSPFv3 > General (Add) page.

■**Path Code Type** – The way these routes were learned. (Displayed entries include: Connected, Discard, OSPF, OSPF inter area, OSPF NSSA external type 1, OSPF NSSA external type 2, OSPF external type 1, OSPF external type 2)

■**IP Address** – The destination IP address and prefix length of this route.

■**Cost** – The cost of sending a protocol packet to a host address or to a subnet indicated by an address prefix.

■**Next Hop Connected** – The next hop IP address of this route. Note that, discarded and directly connected routes have no next hops, and are displayed as 0.0.0.0.

■**Next Hop Name** – The name of outgoing interface which links to next hop.

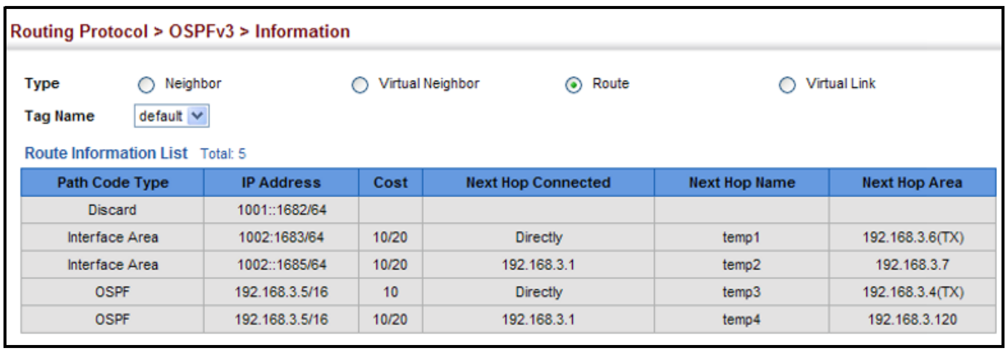
■**Next Hop Area** – The OSPFv3 area in which the next hop router resides. Note that, discarded and external routes have no area option for the path, and always return 0.0.0.0. This field will also include a “(TX)” suffix if the entry is a transit area.

### WEB INTERFACE

To display the OSPFv3 routing table:

1. Click Routing Protocol, OSPFv3, Information.
2. Click Route.
3. Select the tag name.

**Figure 79: Displaying the OSPFv3 Routing Table**




| Path Code Type | IP Address | Cost | Next Hop Connected | Next Hop Name | Next Hop Area |
|---|---|---|---|---|---|
| Discard | 1001::1682/64 | | | | |
| Interface Area | 1002:1683/64 | 10/20 | Directly | temp1 | 192.168.3.6(TX) |
| Interface Area | 1002::1685/64 | 10/20 | 192.168.3.1 | temp2 | 192.168.3.7 |
| OSPF | 192.168.3.5/16 | 10 | Directly | temp3 | 192.168.3.4(TX) |
| OSPF | 192.168.3.5/16 | 10/20 | 192.168.3.1 | temp4 | 192.168.3.120 |

## DISPLAYING INFORMATION ON VIRTUAL LINKS

Use the Routing Protocol > OSPFv3 > Information (Virtual Link) page to show the Link State Advertisements (LSAs) stored in the link state database for virtual links.

### CLI REFERENCES

■"show ipv6 ospf virtual-links" on page 1200

### PARAMETERS

These parameters are displayed in the web interface:

■**Tag Name** – A process name as configured on the Routing Protocol > OSPFv3 > General (Add) page.

■**Name** – Index for this table entry.

■**Router ID** – Virtual neighbor’s router ID.

■**Status** – Indicates if the link is up or down.

■**Transit Area** – Common area the virtual link crosses to reach the target router. This identifier is in the form of an IP address.

■**Local Address** – The IP address of ABR that serves as an endpoint connecting the isolated area to the common transit area.

- **Remote Address** – The IP address this virtual neighbor is using. The neighbor must be an ABR at the other endpoint connecting the common transit area to the backbone itself.

- **State** – The interface status for a virtual link:
  - Disabled – OSPF not enabled on this interface
  - Down – OSPF is enabled on this interface, but interface is down
  - Loopback – This is a loopback interface
  - Waiting – Router is trying to find the DR and BDR
  - DR – Designated Router
  - BDR – Backup Designated Router
  - DROther – Interface is on a multiaccess network, but is not the DR or BDR

- **Hello Due** – The number of seconds before the next hello message is due. This time is determined by the Hello Interval which must be the same for all router attached to a common network.

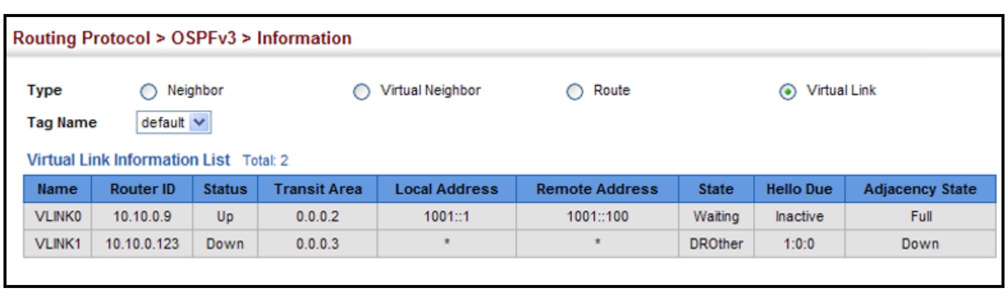
- **Adjancy State** – The adjancy state of the virtual neighbor relationship:
  - Down – Connection down
  - Attempt – Connection down, but attempting contact (non-broadcast networks)
  - Init – Have received Hello packet, but communications not yet established
  - Two-way – Bidirectional communications established
  - ExStart – Initializing adjacency between neighbors
  - Exchange – Database descriptions being exchanged
  - Loading – LSA databases being exchanged
  - Full – Neighboring routers now fully adjacent

### WEB INTERFACE

To display information about virtual links stored in the link state database:

1. Click Routing Protocol, OSPF, Information.
2. Click Virtual Link.
3. Select the process identifier.

**Figure 80: Displaying Virtual Links Stored in the Link State Database**




| Name | Router ID | Status | Transit Area | Local Address | Remote Address | State | Hello Due | Adjacency State |
|---|---|---|---|---|---|---|---|---|
| VLINK0 | 10.10.0.9 | Up | 0.0.0.2 | 1001::1 | 1001::100 | Waiting | Inactive | Full |
| VLINK1 | 10.10.0.123 | Down | 0.0.0.3 | * | * | DROther | 1:0:0 | Down |

# 22 MULTICAST ROUTING

This chapter describes the following multicast routing topics:

- Enabling Multicast Routing Globally – Describes how to globally enable multicast routing.
- Displaying the Multicast Routing Table – Describes how to display the multicast routing table.
- Configuring PIM for IPv4 – Describes how to configure PIM-DM and PIM-SM for IPv4.
- Configuring PIMv6 for IPv6 – Describes how to configure PIM-DM (Version 6) for IPv6.

## OVERVIEW

This router can route multicast traffic to different subnetworks using Protocol-Independent Multicasting - Dense Mode or Sparse Mode (PIM-DM or PIM-SM) for IPv4, as well as PIM-DM for IPv6. PIM for IPv4 (also called PIMv4 in this manual) relies on messages sent from IGMP-enabled Layer 2 switches and hosts to determine when hosts want to join or leave multicast groups. PIM for IPv6 (also called PIMv6 in this manual) uses the Multicast Listener Discovery (MLDv1) protocol which is the IPv6 equivalent to IGMPv2. PIM-DM is designed for networks where the probability of multicast group members is high, such as a local network. PIM-SM is designed for networks where the probability of multicast group members is low, such as the Internet.

Also, note that if PIM is not enabled on this router or another multicast routing protocol is used on the network, the switch ports attached to a multicast router can be manually configured to forward multicast traffic (see "Specifying Static Interfaces for a Multicast Router" on page 382).

*Configuring PIM-DM*

PIM-DM floods multicast traffic downstream, and calculates the shortest-path, source-rooted delivery tree between each source and destination host group. Other multicast routing protocols, such as DVMRP, build their own source-rooted multicast delivery tree (i.e., a separate routing table) that allows it to prevent looping and determine the shortest path to the source of the multicast traffic. PIM-DM also builds a source-rooted multicast delivery tree for each multicast source, but uses information from the router's unicast routing table, instead of maintaining its own multicast routing table, making it routing protocol independent.

PIM-DM is a simple multicast routing protocol that uses flood and prune to build a source-routed multicast delivery tree for each multicast source-group pair. As mentioned above, it does not maintain it's own routing table, but instead, uses the routing table provided by whatever unicast routing protocol is enabled on the router interface. When the router receives a multicast packet for a source-group pair, PIM-DM checks the unicast routing table on the inbound interface to determine if this is the same interface used for routing unicast packets to the multicast source network. If it is not, the router drops the packet and sends an Assert message back out the source interface. An Assert winner is then selected to continue forwarding traffic from this source. On the other hand, if it is the same interface used by the unicast protocol, then the router forwards a copy of the packet to all the other interfaces for which is has not already received a prune message for this specific source-group pair.

DVMRP holds the prune state for about two hours, while PIM-DM holds it for only about three minutes. Although this results in more flooding than encountered with DVMRP, this is the only major trade-off for the lower processing overhead and simplicity of configuration for PIM-DM.

*Configuring PIM-SM*

PIM-SM uses the router's local unicast routing table to route multicast traffic, not to flood it. It only forwards multicast traffic when requested by a local or downstream host. When service is requested by a host, it can use a Reverse Path Tree (RPT) that channels the multicast traffic from each source through a single Rendezvous Point (RP) within the local PIM-SM domain, and then forwards this traffic to the Designated Router (DR) in the local network segment to which the host is attached. However, when the multicast load from a particular source is heavy enough to justify it, PIM-SM can be configured to construct a Shortest Path Tree (SPT) directly from the DR up to the source, bypassing the RP and thereby reducing service delays for active hosts and setup time for new hosts.

PIM-SM reduces the amount of multicast traffic by forwarding it only to the ports that are attached to receivers for a group. The key components to filtering multicast traffic are listed below.

**Common Domain** – A common domain must be set up in which all of the multicast routers are configured with the same basic PIM-SM settings.

**Bootstrap Router** (BSR) – After the common domain is set, a bootstrap router is elected from this domain. Each time a PIM-SM router is booted up, or the multicast mode reconfigured to enable PIM-SM, the bootstrap router candidates start flooding bootstrap messages on all of their interfaces (using reverse path forwarding to limit the impact on the network). When neighboring routers receive bootstrap messages, they process the message and forward it out through all interfaces, except for the interface on which this message was received. If a router receives a bootstrap message with a BSR priority larger than its own, it stops advertising itself as a BSR candidate. Eventually, only the router with the highest BSR priority will continue sending bootstrap messages.

**Rendezvous Point** (RP) – A router may periodically sends PIMv2 messages to the BSR advertising itself as a candidate RP for specified group addresses. The BSR places information about all of the candidate RPs in subsequent bootstrap messages. The BSR and all the routers receiving these messages use the same hash algorithm to elect an RP for each multicast group. If each router is properly configured, the results of the election process will be the same for each router. Each elected RP then starts to serve as the root of a shared distribution tree for one or more multicast groups.

**Designated Router** (DR) – A DR advertising the highest priority in its hello messages is elected for each subnet. The DR is responsible for collecting information from the subnet about multicast clients that want to join or leave a group. Join messages from the DR (receiver) for each group are sent towards the RP, and data from multicast sources is sent to the RP. Receivers can now start receiving traffic destined for the client group from the RP, or they can identify the senders and optionally set up a direct connection to the source through a shortest path tree (SPT) if the loading warrants this change over.

**Shared Tree** – When many receivers join a group, their Join messages converge on the RP, and form a distribution tree for the group that is rooted at the RP. This is known as the Reverse Path Tree (RPT), or the shared tree since it is shared by all sources sending to that group. When a multicast source sends data destined for a group, the source's local DR takes those data packets, unicast-encapsulates them, and sends them to the RP. When the RP receives these encapsulated data packets, it decapsulates them, and forwards them onto the shared tree. These packets follow the group mapping maintained by routers along the RP Tree, are replicated wherever the RP Tree branches, and eventually reach all the receivers for that multicast group. Because all routers along the shared tree are using PIM-SM, the multicast flow is confined to the shared tree. Also, note that more than one flow can be carried over the same shared tree, but only one RP is responsible for each flow.

**Shortest Path Tree** (SPT) – When using the Shared Tree, multicast traffic is contained within the shared tree. However, there are several drawbacks to using the shared tree. Decapsulation of traffic at the RP into multicast packets is a resource intensive process. The protocol does not take into account the location of group members when selecting the RP, and the path from the RP to the receiver is not always optimal. Moreover, a high degree of latency may occur for hosts wanting to join a group because the RP must wait for a register message from the DR before setting up the shared tree and establishing a path back to the source. There is also a problem with bursty sources. When a source frequently times out, the shared tree has to be rebuilt each time, causing further latency in sending traffic to the receiver. To enhance overall network performance, the switch uses the RP only to forward the first packet from a source to the receivers. After the first packet, it calculates the shortest path between the receiver and source and uses the SPT to send all subsequent packets from the source directly to the receiver. When the first packet arrives natively through the shortest path, the RP sends a register-stop message back to the DR near the source. When this DR receives the register-stop message, it stops sending register messages to the RP. If there are no other sources using the shared tree, it is also torn down. Setting up the SPT requires more memory than when using the shared tree, but can significantly reduce group join and data transmission delays. The switch can also be configured to use SPT only for specific multicast groups, or to disable the change over to SPT for specific groups.

## CONFIGURING GLOBAL SETTINGS FOR MULTICAST ROUTING

To use multicast routing on this router, first globally enable multicast routing as described in this section, then specify the interfaces that will employ multicast routing protocols (PIM-DM or PIM-SM for IPv4 on page 572, or PIM-DM for IPv6 on page 587). Note that only one IPv4 multicast routing protocol (PIM-DM or PIM-SM) can be enabled on any given interface, but both PIMv4 and PIMv6 can be enabled on the same interface.

### Enabling Multicast Routing Globally

Use the Multicast > Multicast Routing > General page to enable IP multicast routing globally on the switch.

#### CLI REFERENCES

- "ip multicast-routing" on page 1201

#### PARAMETERS

These parameters are displayed in the web interface:

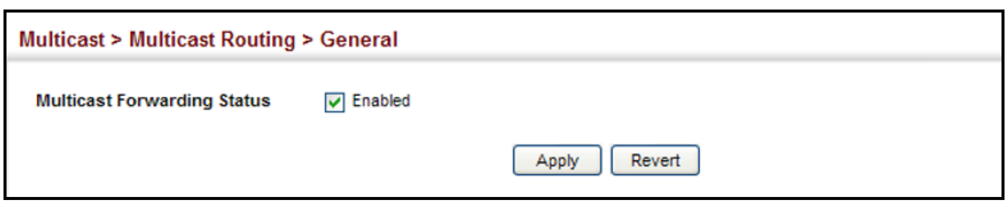
- **Multicast Forwarding Status** – Enables IP multicast routing. (Default: Disabled)

#### WEB INTERFACE

To enable multicast routing:

1. Click Multicast, Multicast Routing, General.
2. Enable Multicast Forwarding Status.
3. Click Apply.

**Figure 1: Enabling Multicast Routing**



## Displaying the Multicast Routing Table

Use the Multicast > Multicast Routing > Information page to display information on each multicast route it has learned through PIM. The router learns multicast routes from neighboring routers, and also advertises these routes to its neighbors. The router stores entries for all paths learned by itself or from other routers, without considering actual group membership or prune messages. The routing table therefore does not indicate that the router has processed multicast traffic from any particular source listed in the table. It uses these routes to forward multicast traffic only if group members appear on directly-attached subnetworks or on subnetworks attached to downstream routers.

### CLI REFERENCES

- "show ip mroute" on page 1202

### PARAMETERS

These parameters are displayed in the web interface:

*Show Summary*

- **Group Address** – IP group address for a multicast service.
- **Source Address** – Subnetwork containing the IP multicast source.
- **Source Mask** – Network mask for the IP multicast source. (Note that the switch cannot detect the source mask, and therefore displays 255.255.255.255 in this field.)
- **Interface** – Upstream interface leading to the upstream neighbor.

  PIM creates a multicast routing tree based on the unicast routing table. If the related unicast routing table does not exist, PIM will still create a multicast routing entry, displaying the upstream interface to indicate that this entry is valid. This field may also display “Register” to indicate that a pseudo interface is being used to receive PIM-SM register packets. This can occur for the Rendezvous Point (RP), which is the root of the Reverse Path Tree (RPT). In this case, any VLAN receiving register packets will be converted into the register interface.
- **Owner** – The associated multicast protocol (PIM-DM, PIM-SM, IGMP Proxy).
- **Flags** – The flags associated with each routing entry indicate:
  - **Forward** – Traffic received from the upstream interface is being forwarded to this interface.
  - **Local** – This is the outgoing interface.
  - **Pruned** – This interface has been pruned by a downstream neighbor which no longer wants to receive the traffic.

*Show Details*

- **Group Address** – IP group address for a multicast service.
- **Source Address** – Subnetwork containing the IP multicast source.

- **Source Mask** – Network mask for the IP multicast source.
- **Upstream Neighbor** – The multicast router (RPF Neighbor) immediately upstream for this group.
- **Upstream Interface** – Interface leading to the upstream neighbor.
- **Up Time** – Time since this entry was created.
- **Owner** – The associated multicast protocol (PIM-DM, PIM-SM, IGMP Proxy).
- **Flags** – The flags associated with each routing entry indicate:
  - **Dense** – PIM Dense mode in use.
  - **Sparse** – PIM Sparse mode in use.
  - **Connected** – This route is directly connected to the source.
  - **Pruned** – This route has been terminated.
  - **Register flag** – This device is registering for a multicast source.
  - **RPT-bit set** – The (S,G) entry is pointing to the Rendezvous Point (RP), which normally indicates a pruned state along the shared tree for a particular source.
  - **SPT-bit set** – Multicast packets have been received from a source on shortest path tree.
  - **Join SPT** – The rate of traffic arriving over the shared tree has exceeded the SPT-threshold for this group. If the SPT flag is set for (*,G) entries, the next (S,G) packet received will cause the router to join the shortest path tree. If the SPT flag is set for (S,G), the router immediately joins the shortest path tree.

Downstream Interface List –

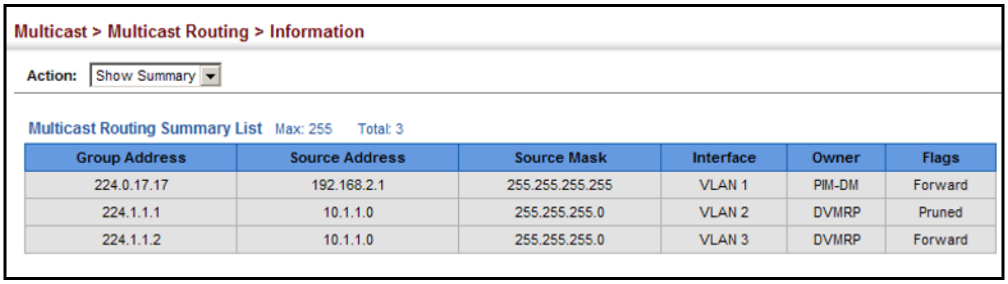
- **Interface** – Interface(s) on which multicast subscribers have been recorded.
- **State** – The flags associated with each downstream interface indicate:
  - **Forward** – Traffic received from the upstream interface is being forwarded to this interface.
  - **Local** – Downstream interface has received IGMP report message from host in this subnet.
  - **Pruned** – This route has been terminated.
  - **Registering** - A downstream device is registering for a multicast source.

**WEB INTERFACE**

To display the multicast routing table:

1. Click Multicast, Multicast Routing, Information.
2. Select Show Summary from the Action List.

**Figure 2: Displaying the Multicast Routing Table**

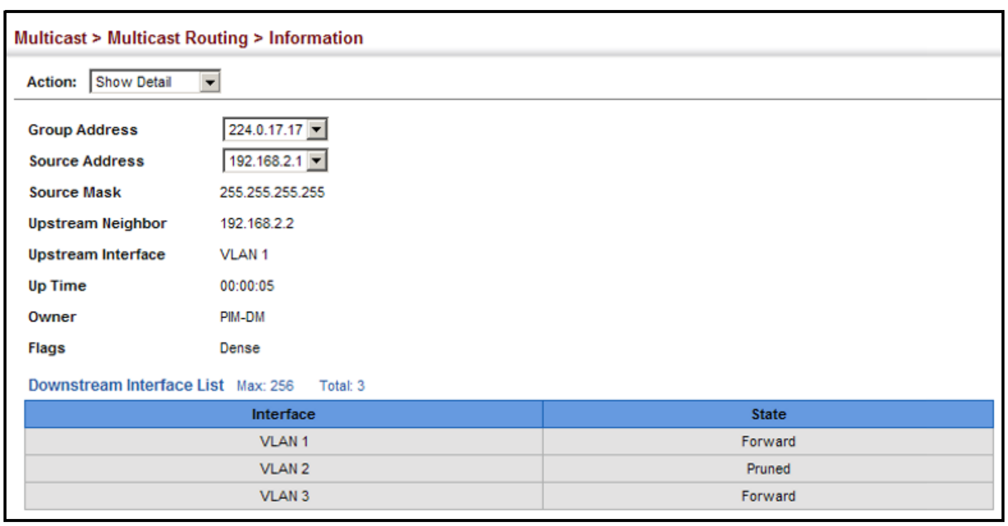



| Group Address | Source Address | Source Mask | Interface | Owner | Flags |
|---|---|---|---|---|---|
| 224.0.17.17 | 192.168.2.1 | 255.255.255.255 | VLAN 1 | PIM-DM | Forward |
| 224.1.1.1 | 10.1.1.0 | 255.255.255.0 | VLAN 2 | DVMRP | Pruned |
| 224.1.1.2 | 10.1.1.0 | 255.255.255.0 | VLAN 3 | DVMRP | Forward |

To display detailed information on a specific flow in multicast routing table:

1. Click Multicast, Multicast Routing, Information.
2. Select Show Details from the Action List.
3. Select a Group Address.
4. Select a Source Address.

**Figure 3: Displaying Detailed Entries from the Multicast Routing Table**




| Interface | State |
|---|---|
| VLAN 1 | Forward |
| VLAN 2 | Pruned |
| VLAN 3 | Forward |

# CONFIGURING PIM FOR IPV4

This section describes how to configure PIM-DM and PIM-SM for IPv4.

## Enabling PIM Globally

Use the Routing Protocol > PIM > General page to enable IPv4 PIM routing globally on the router.

### CLI REFERENCES

- "router pim" on page 1209

### COMMAND USAGE

- This feature enables PIM-DM and PIM-SM globally for the router. You also need to enable PIM-DM or PIM-SM for each interface that will support multicast routing (see page 572), and make any changes necessary to the multicast protocol parameters.
- To use PIM, multicast routing must be enabled on the switch (see "Enabling Multicast Routing Globally" on page 568).

### WEB INTERFACE

To enable PIM multicast routing:

1. Click Routing Protocol, PIM, General.
2. Enable PIM Routing Protocol.
3. Click Apply.

**Figure 4: Enabling PIM Multicast Routing**


## Configuring PIM Interface Settings

Use the Routing Protocol > PIM > Interface page configure the routing protocol's functional attributes for each interface.

### CLI REFERENCES

- "IPv4 PIM Commands" on page 1208

### COMMAND USAGE

- Most of the attributes on this page are common to both PIM-DM and PIM-SM. Select Dense or Sparse Mode to display the common attributes, as well as those applicable to the selected mode.

- PIM and IGMP proxy cannot be used at the same time. When an interface is set to use PIM Dense mode or Sparse mode, IGMP proxy cannot be enabled on any interface of the device (see "Configuring IGMP Snooping and Query Parameters" on page 379). Also, when IGMP proxy is enabled on an interface, PIM cannot be enabled on any interface.

*PIM-DM*

- PIM-DM functions similar to DVMRP by periodically flooding the network with traffic from any active multicast server. It also uses IGMP to determine the presence of multicast group members. The main difference, is that it uses the router's unicast routing table to determine if the interface through which a packet is received provides the shortest path back to the source.

- Dense-mode interfaces are subject to multicast flooding by default, and are only removed from the multicast routing table when the router determines that there are no group members or downstream routers, or when a prune message is received from a downstream router.

*PIM-SM*

- A PIM-SM interface is used to forward multicast traffic only if a join message is received from a downstream router or if group members are directly connected to the interface. When routers want to receive a multicast flow, they periodically send join messages to the RP, and are subsequently added to the shared path for the specified flow back up to the RP. If routers want to join the source path up through the SPT, they periodically send join messages toward the source. They also send prune messages toward the RP to prune the shared path once they have connected to the source through the SPT, or if there are no longer any group members connected to the interface.

### PARAMETERS

These parameters are displayed in the web interface:

*Common Attributes*

- **VLAN** – Layer 3 VLAN interface. (Range: 1-4093)

- **Mode** – PIM routing mode. (Options: Dense, Sparse, None)

- **IP Address** – Primary IP address assigned to the selected VLAN.

- **Hello Holdtime** – Sets the interval to wait for hello messages from a neighboring PIM router before declaring it dead. Note that the hello holdtime should be greater than or equal to the value of Hello Interval, otherwise it will be automatically set to 3.5 x the Hello Interval. (Range: 1-65535 seconds; Default: 105 seconds, or 3.5 times the hello interval if set)

- **Hello Interval** – Sets the frequency at which PIM hello messages are transmitted out on all interfaces. (Range: 1-65535 seconds; Default: 30 seconds)

  Hello messages are sent to neighboring PIM routers from which this device has received probes, and are used to verify whether or not these neighbors are still active members of the multicast tree. PIM-SM routers use these messages not only to inform neighboring routers of their presence, but also to determine which router for each LAN segment will serve as the Designated Router (DR).

When a router is booted or first configured to use PIM, it sends an initial hello message, and then sets its Hello timer to the configured value. If a router does not hear from a neighbor for the period specified by the Hello Holdtime, that neighbor is dropped. This hold time is included in each hello message received from a neighbor. Also note that hello messages also contain the DR priority of the router sending the message.

If the hello holdtime is already configured, and the hello interval is set to a value longer than the hello holdtime, this command will fail.

- **Join/Prune Holdtime** – Sets the hold time for the prune state. (Range: 1-65535 seconds; Default: 210 seconds)
  - PIM-DM: The multicast interface that first receives a multicast stream from a particular source forwards this traffic to all other PIM-DM interfaces on the router. If there are no requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The prune state is maintained until the join/prune holdtime timer expires or a graft message is received for the forwarding entry.
  - PIM-SM: The multicast interface that first receives a multicast stream from a particular source forwards this traffic only to those interfaces on the router that have requests to join this group. When there are no longer any requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The protocol maintains both the current join state and the pending RPT prune state for this (source, group) pair until the join/prune interval timer expires.
- **LAN Prune Delay** – Causes this device to inform downstream routers of how long it will wait before pruning a flow after receiving a prune request. (Default: Disabled)

  When other downstream routers on the same VLAN are notified that this upstream router has received a prune request, they must send a Join to override the prune before the prune delay expires if they want to continue receiving the flow. The message generated by this command effectively prompts any downstream neighbors with hosts receiving the flow to reply with a Join message. If no join messages are received after the prune delay expires, this router will prune the flow.

  The sum of the Override Interval and Propagation Delay are used to calculate the LAN prune delay.
- **Override Interval** – The time required for a downstream router to respond to a LAN Prune Delay message by sending back a Join message if it wants to continue receiving the flow referenced in the message. (Range: 500-6000 milliseconds; Default: 2500 milliseconds)

  The override interval and the propagation delay are used to calculate the LAN prune delay. If a downstream router has group members which want to continue receiving the flow referenced in a LAN prune delay message, then the override interval represents the time required for the downstream router to process the message and then respond by sending a Join message back to the upstream router to ensure that the flow is not terminated.
- **Propagation Delay** – The time required for a LAN prune delay message to reach downstream routers. (Range: 100-5000 milliseconds; Default: 500 milliseconds)

The override interval and pro po gat ion delay are used to calculate the LAN prune delay. If a downstream router has group members which want to continue receiving the flow referenced in a LAN prune delay message, then the propagation delay represents the time required for the LAN prune delay message to be propagated down from the upstream router to all downstream routers attached to the same VLAN interface.

- **Trigger Hello Delay** – The maximum time before transmitting a triggered PIM Hello message after the router is rebooted or PIM is enabled on an interface. (Range: 0-5 seconds; Default: 5 seconds)

  When a router first starts or PIM is enabled on an interface, the hello delay is set to random value between 0 and the trigger hello delay. This prevents synchronization of Hello messages on multi-access links if multiple routers are powered on simultaneously.

  Also, if a Hello message is received from a new neighbor, the receiving router will send its own Hello message after a random delay between 0 and the trigger hello delay.

*Dense-Mode Attributes*

- **Graft Retry Interval** – The time to wait for a Graft acknowledgement before resending a Graft message. (Range: 1-10 seconds; Default: 3 seconds)

  A graft message is sent by a router to cancel a prune state. When a router receives a graft message, it must respond with an graft acknowledgement message. If this acknowledgement message is lost, the router that sent the graft message will resend it a number of times (as defined by Max. Graft Retries).

- **Max. Graft Retries** – The maximum number of times to resend a Graft message if it has not been acknowledged. (Range: 1-10; Default: 3)

- **State Refresh Origination Interval** – The interval between sending PIM-DM state refresh control messages. (Range: 1-100 seconds; Default: 60 seconds)

  The pruned state times out approximately every three minutes and the entire PIM-DM network is reflooded with multicast packets and prune messages. The state refresh feature keeps the pruned state from timing out by periodically forwarding a control message down the distribution tree, refreshing the prune state on the outgoing interfaces of each router in the tree. This also enables PIM routers to recognize topology changes (sources joining or leaving a multicast group) before the default three-minute state timeout expires.

  This command is only effectively for interfaces of first hop, PIM-DM routers that are directly connected to the sources of multicast groups.

*Sparse-Mode Attributes*

- **DR Priority** – Sets the priority advertised by a router when bidding to become the Designated Router (DR). (Range: 0-4294967294; Default: 1)

  More than one PIM-SM router may be connected to an Ethernet or other shared-media LAN. If multicast hosts are directly connected to the LAN, then only one of these routers is elected as the DR, and acts on behalf of these hosts, sending periodic Join/Prune messages toward a group-specific RP for each group. A single DR is elected per interface (LAN or otherwise) using a simple election process.

The router with the highest priority configured on an interface is elected as the DR. If more than one router attached to this interface uses the same priority, then the router with the highest IP address is elected to serve as the DR.

If a router does not advertise a priority in its hello messages, it is assumed to have the highest priority and is elected as the DR. If more than one router is not advertising its priority, then the router with the highest IP address is elected to serve as the DR.

- **Join/Prune Interval** – Sets the interval at which join/prune messages are sent. (Range: 1-65535 seconds; Default: 60 seconds)

  By default, the switch sends join/prune messages every 60 seconds to inform other PIM-SM routers about clients who want to join or leave a multicast group.

  Use the same join/prune message interval on all PIM-SM routers in the same PIM-SM domain, otherwise the routing protocol's performance will be adversely affected.

  The multicast interface that first receives a multicast stream from a particular source forwards this traffic only to those interfaces on the router that have requests to join this group. When there are no longer any requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The protocol maintains both the current join state and the pending RPT prune state for this (source, group) pair until the join/prune interval timer expires.

#### WEB INTERFACE

To configure PIM interface settings:

1. Click Routing Protocol, PIM, Interface.
2. Modify any of the protocol parameters as required.
3. Click Apply.

**Figure 5: Configuring PIM Interface Settings** (Dense Mode)

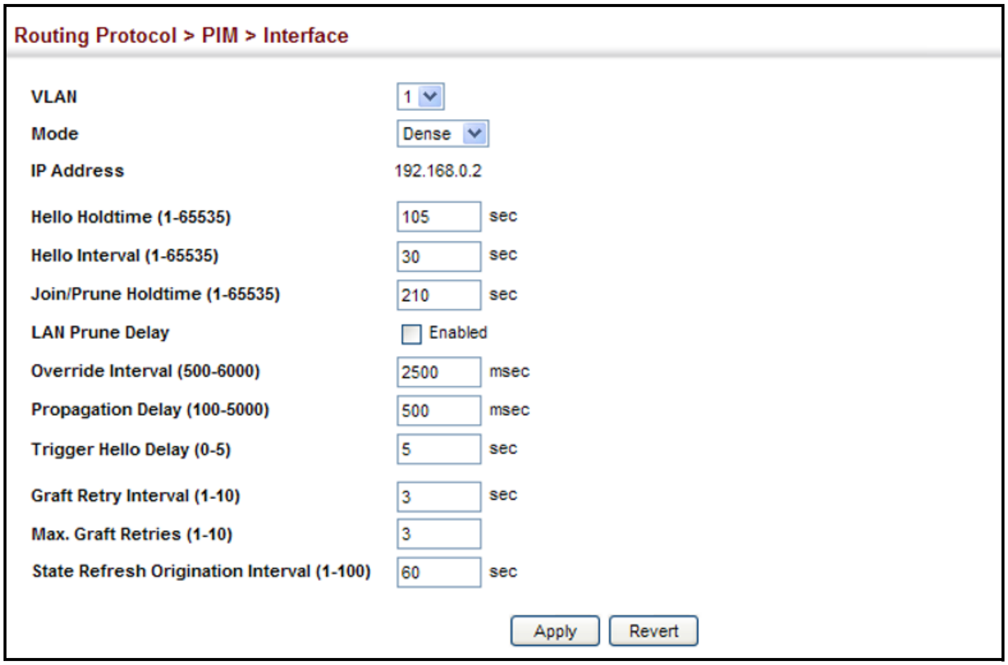
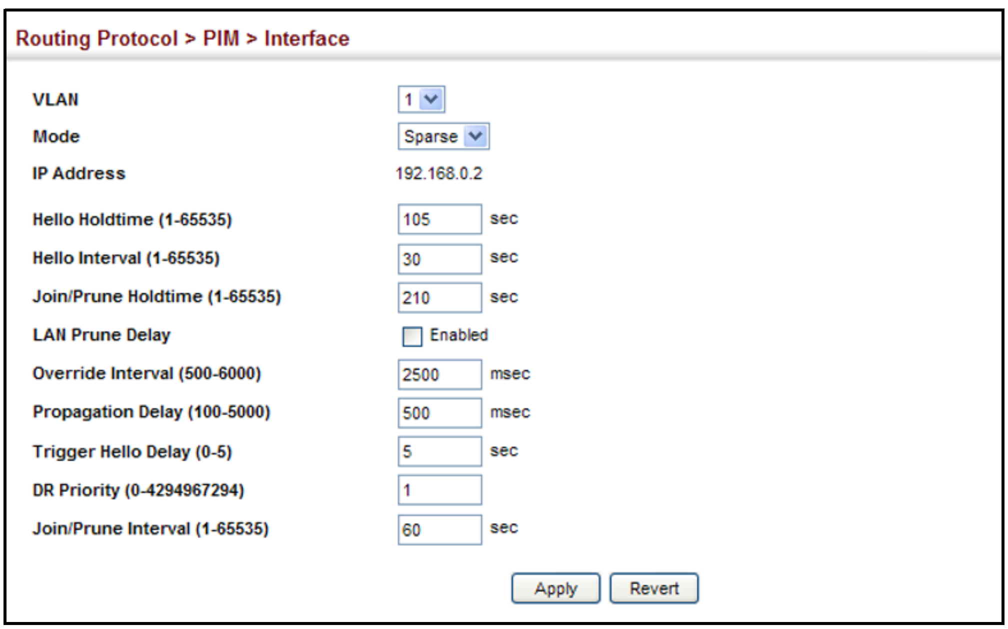



**Figure 6: Configuring PIM Interface Settings** (Sparse Mode)



## Displaying Neighbor Information

Use the Routing Protocol > PIM > Neighbor page to display all neighboring PIM routers.

### CLI REFERENCES

■ "show ip pim neighbor" on page 1216

### PARAMETERS

These parameters are displayed in the web interface:

■ **Address** – IP address of the next-hop router.

■ **VLAN** – VLAN that is attached to this neighbor.

■ **Uptime** – The duration this entry has been active.

■ **Expire** – The time before this entry will be removed.

### WEB INTERFACE

To display neighboring PIM routers:

1. Click Routing Protocol, PIM, Neighbor.

**Figure 7: Showing PIM Neighbors**

Routing Protocol > PIM > Neighbor

Neighbor Information Max: 128 Total: 2

| Address | VLAN | Uptime | Expire |
|---|---|---|---|
| 10.1.2.50 | 1 | 00:01:23 | 00:01:23 |
| 10.1.2.51 | 2 | 1d11h | Never |

## Configuring Global PIM-SM Settings

Use the Routing Protocol > PIM > SM (Configure Global) page to configure the rate at which register messages are sent, the source of register messages, and switchover to the Shortest Path Tree (SPT).

### CLI REFERENCES

■ "IPv4 PIM Commands" on page 1208

### PARAMETERS

These parameters are displayed in the web interface:

■ **Register Rate Limit** – Configures the rate at which register messages are sent by the Designated Router (DR) for each (source, group) entry. (Range: 1-65535 packets per second: Default: disabled)

This parameter can be used to relieve the load on the designated router (DR) and rendezvous point (RP). However, because register messages exceeding the limit are dropped, some receivers may experience data packet loss within the first few seconds in which register messages are sent from bursty sources.

■ **Register Source** – Configures the IP source address of a register message to an address other than the outgoing interface address of the DR that leads back toward the RP. (Range: VLAN 1-4094; Default: The IP address of the DR's outgoing interface that leads back to the RP)

When the source address of a register message is filtered by intermediate network devices, or is not a uniquely routed address to which the RP can send packets, the replies sent from the RP to the source address will fail to reach the DR, resulting in PIM-SM protocol failures. This type of problem can be overcome by manually configuring the source address of register messages to an interface that leads back to the RP.

- **SPT Threshold** – Prevents the last-hop PIM-SM router from switching to Shortest Path Source Tree (SPT) mode. (Options: Infinity, Reset; Default: Reset, or use the SPT)

  The default path for packets from a multicast source to a receiver is through the RP. However, the path through the RP is not always the shortest path. Therefore, the router uses the RP to forward only the first packet from a new multicast group to its receivers. Afterwards, it calculates the shortest path tree (SPT) directly between the receiver and source, and then uses the SPT to send all subsequent packets from the source to the receiver instead of using the shared tree. Note that when the SPT threshold is not set by this command, the PIM leaf router will join the shortest path tree immediately after receiving the first packet from a new source.

  Enable the SPT threshold to force the router to use the shared tree for all multicast groups, or just for the specified multicast groups.

- **Group Address** – An IP multicast group address. If a group address is not specified, the shared tree is used for all multicast groups.

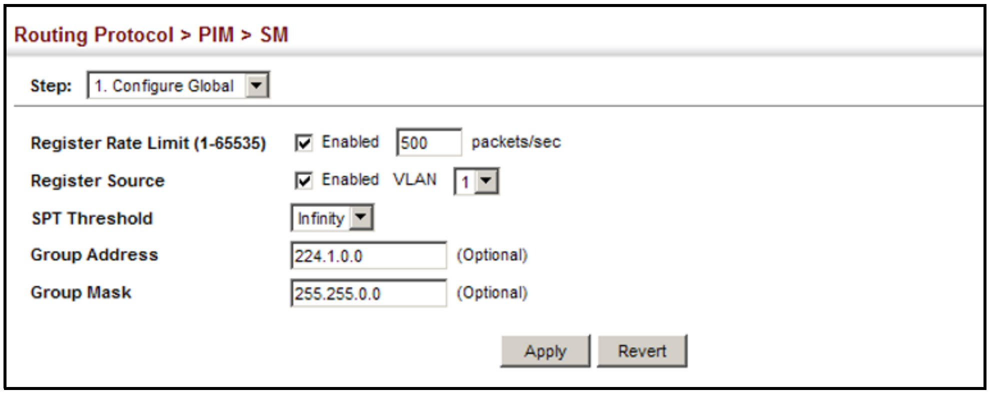
- **Group Mask** – Subnet mask that is used for the group address.

### WEB INTERFACE

To configure global settings for PIM-SM:

1. Click Multicast, Multicast Routing, SM.
2. Select Configure Global from the Step list.
3. Set the register rate limit and source of register messages if required. Also specify any multicast groups which must be routed across the shared tree, instead of switching over to the SPT.
4. Click Apply.

**Figure 8: Configuring Global Settings for PIM-SM**




## Configuring a BSR Candidate

Use the Routing Protocol > PIM > SM (BSR Candidate) page to configure the switch as a Bootstrap Router (BSR) candidate.

### CLI REFERENCES

- "ip pim bsr-candidate" on page 1219

### COMMAND USAGE

- When this router is configured as a BSR candidate, it starts sending bootstrap messages to all of its PIM-SM neighbors. The primary IP address of the designated VLAN is sent as the candidate's BSR address. Each neighbor receiving the bootstrap message compares the BSR address with the address from previous messages. If the current address is the same or a higher address, it accepts the bootstrap message and forwards it. Otherwise, it drops the message.

- This router will continue to be the BSR until it receives a bootstrap message from another candidate with a higher priority (or a higher IP address if the priorities are the same).

- To improve failover recovery, it is advisable to select at least two core routers in diverse locations, each to serve as both a candidate BSR and candidate RP. It is also preferable to set up one of these routers as both the primary BSR and RP.

### PARAMETERS

These parameters are displayed in the web interface:

- **BSR Candidate Status** – Configures the switch as a Bootstrap Router (BSR) candidate. (Default: Disabled)

- **VLAN ID** – Identifier of configured VLAN interface. (Range: 1-4093)

- **Hash Mask Length** – Hash mask length (in bits) used for RP selection (see "Configuring a Static Rendezvous Point" on page 581 and "Configuring an RP Candidate" on page 583). The portion of the hash specified by the mask length is ANDed with the group address. Therefore, when the hash function is executed on any BSR, all groups with the same seed hash will be mapped to the same RP. If the mask length is less than 32, then only the first portion of the hash is used, and a single RP will be defined for multiple groups. (Range: 0-32; Default: 10)

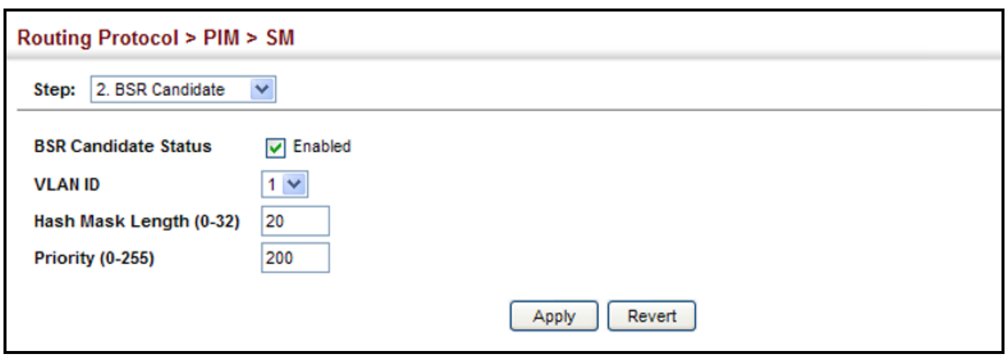
■**Priority** – Priority used by the candidate bootstrap router in the election process. The BSR candidate with the largest priority is preferred. If the priority values are the same, the candidate with the larger IP address is elected to be the BSR. Setting the priority to zero means that this router is not eligible to server as the BSR. At least one router in the PIM-SM domain must be set to a value greater than zero. (Range: 0-255; Default: 0)

### WEB INTERFACE

To configure the switch as a BSR candidate:

1. Click Multicast, Multicast Routing, SM.
2. Select BSR Candidate from the Step list.
3. Specify the VLAN interface for which this router is bidding to become the BSR, the hash mask length that will subsequently be used for RP selection if this router is selected as the BSR, and the priority for BSR selection.
4. Click Apply.

**Figure 9: Configuring a BSR Candidate**




## Configuring a Static Rendezvous Point

Use the Routing Protocol > PIM > SM (RP Address) page to configure a static address as the Rendezvous Point (RP) for a particular multicast group.

### CLI REFERENCES

■"ip pim rp-address" on page 1221

### COMMAND USAGE

■The router will act as an RP for all multicast groups in the local PIM-SM domain if no groups are specified. A static RP can either be configured for the whole multicast group range 224/4, or for specific group ranges.

■If an IP address is specified that was previously used for an RP, then the older entry is replaced.

■Multiple RPs can be defined for different groups or group ranges. If a group is matched by more than one entry, the router will use the RP associated with the longer group prefix length. If the prefix lengths are the same, then the static RP with the highest IP address is chosen.

- Static definitions for RP addresses may be used together with RP addresses dynamically learned through the bootstrap router (BSR). If an RP address learned by the BSR and one statically configured using this command are both available for a group range, the RP address learned by the BSR is chosen over the one statically configured.

- All routers within the same PIM-SM domain must be configured with the same RP(s). Selecting an RP through the dynamic election process is therefore preferable for most situations. Using the dynamic RP election process also allows a backup RP to automatically take over if the active RP router becomes unavailable.

### PARAMETERS

These parameters are displayed in the web interface:

- **RP Address** – Static IP address of the router that will be an RP for the specified multicast group(s).

- **Group Address** – An IP multicast group address. If a group address is not specified, the RP is used for all multicast groups.

- **Group Mask** – Subnet mask that is used for the group address.

### WEB INTERFACE

To configure a static rendezvous point:

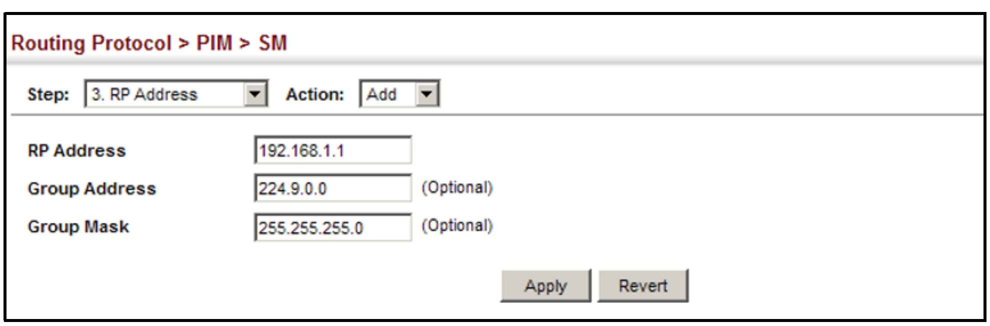
1. Click Multicast, Multicast Routing, SM.

2. Select RP Address from the Step list.

3. Specify the static RP to use for a multicast group, or a range of groups by using a subnet mask.

4. Click Apply.

**Figure 10: Configuring a Static Rendezvous Point**



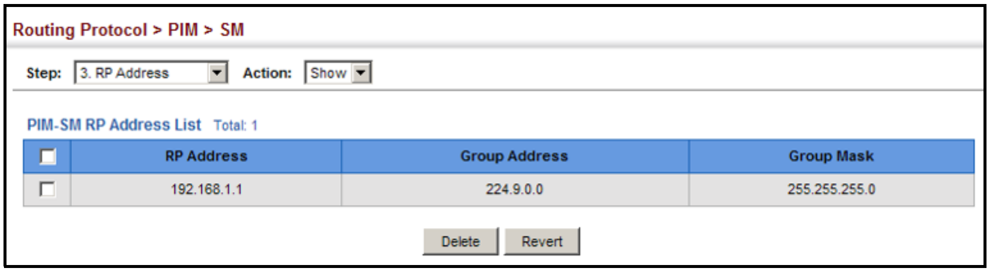

To display static rendezvous points:

1. Click Multicast, Multicast Routing, SM.

2. Select RP Address from the Step list.

**3.** Select Show from the Action list.

**Figure 11: Showing Static Rendezvous Points**




## Configuring an RP Candidate

Use the Routing Protocol > PIM > SM (RP Candidate) page to configure the switch to advertise itself as a Rendezvous Point (RP) candidate to the bootstrap router (BSR).

### CLI REFERENCES

- "ip pim rp-candidate" on page 1223

### COMMAND USAGE

- When this router is configured as an RP candidate, it periodically sends PIMv2 messages to the BSR advertising itself as a candidate RP for the specified group addresses. The IP address of the designated VLAN is sent as the candidate's RP address. The BSR places information about all of the candidate RPs in subsequent bootstrap messages. The BSR uses the RP-election hash algorithm to select an active RP for each group range. The election process is performed by the BSR only for its own use. Each PIM-SM router that receives the list of RP candidates from the BSR also elects an active RP for each group range using the same election process.

- The election process for each group is based on the following criteria:

  - Find all RPs with the most specific group range.
  - Select those with the highest priority (lowest priority value).
  - Compute hash value based on the group address, RP address, priority, and hash mask included in the bootstrap messages.
  - If there is a tie, use the candidate RP with the highest IP address.

- This distributed election process provides faster convergence and minimal disruption when an RP fails. It also serves to provide load balancing by distributing groups across multiple RPs. Moreover, when an RP fails, the responsible RPs are re-elected on each router, and the groups automatically distributed to the remaining RPs.

- To improve failover recovery, it is advisable to select at least two core routers in diverse locations, each to serve as both a candidate BSR and candidate RP. It is also preferable to set up one of these routers as both the primary BSR and RP.

### PARAMETERS

These parameters are displayed in the web interface:

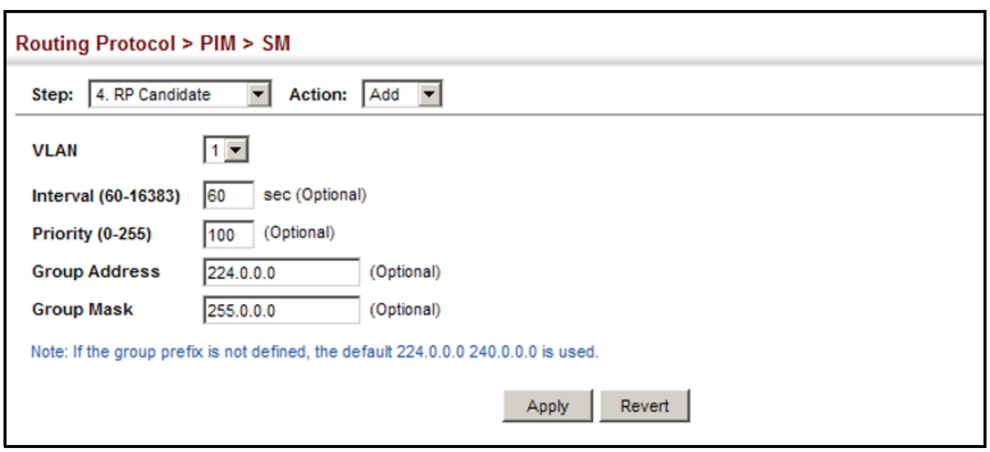
- **VLAN** – Identifier of configured VLAN interface. (Range: 1-4093)
- **Interval** – The interval at which this device advertises itself as an RP candidate. (Range: 60-16383 seconds; Default: 60 seconds)
- **Priority** – Priority used by the candidate RP in the election process. The RP candidate with the largest priority is preferred. If the priority values are the same, the candidate with the larger IP address is elected to be the RP. Setting the priority to zero means that this router is not eligible to server as the RP. (Range: 0-255; Default: 0)
- **Group Address** – An IP multicast group address.
- **Group Mask** – Subnet mask that is used for the group address.

### WEB INTERFACE

To advertise the switch as an RP candidate:

1. Click Multicast, Multicast Routing, SM.
2. Select RP Candidate from the Step list.
3. Specify a VLAN interface, the interval at which to advertise the router as an RP candidate, the priority to use in the election process, and the multicast group address and mask indicating the groups for which this router is bidding to become the RP.
4. Click Apply.

**Figure 12: Configuring an RP Candidate**



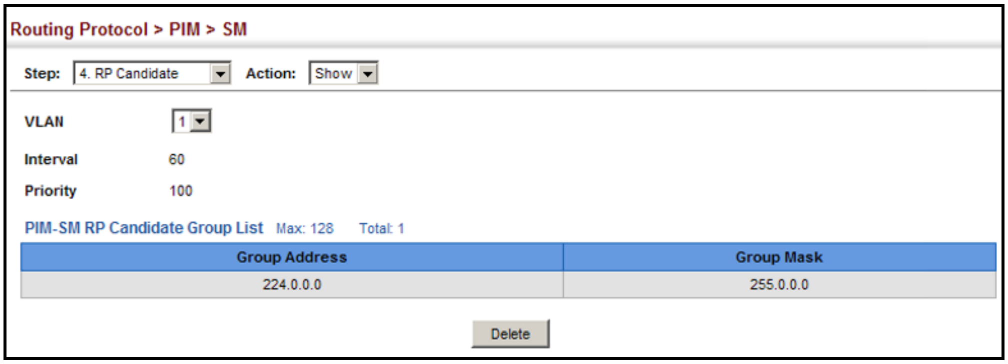

To display settings for an RP candidate:

1. Click Multicast, Multicast Routing, PIM-SM.
2. Select RP Candidate from the Step list.

3. Select Show from the Action list.

4. Select an interface from the VLAN list.

**Figure 13: Showing Settings for an RP Candidate**




## Displaying the BSR Router

Use the Routing Protocol > PIM > SM (Show Information – Show BSR Router) page to display Information about the bootstrap router (BSR).

### CLI REFERENCES

- "show ip pim bsr-router" on page 1227

### PARAMETERS

These parameters are displayed in the web interface:

- **IP Address** – IP address of interface configured as the BSR.
- **Uptime** – The time this BSR has been up and running.
- **Priority** – Priority value used by this BSR candidate.
- **Hash Mask Length** – The number of significant bits used in the multicast group comparison mask by this BSR candidate.
- **Expire** – The time before the BSR is declared down.
- **Role** – Candidate or non-candidate BSR.
- **State**[1] – Operation state of BSR includes:
  - No information – No information is stored for this device.
  - Accept Any – The router does not know of an active BSR, and will accept the first bootstrap message it sees as giving the new BSR's identity and the RP-set.
  - Accept Preferred – The router knows the identity of the current BSR, and is using the RP-set provided by that BSR. Only bootstrap messages from that

1. These parameters are based on RFC 5059.

BSR or from a C-BSR with higher weight than the current BSR will be accepted.

◆ Candidate BSR – Bidding in election process.

◆ Pending-BSR – The router is a candidate to be the BSR for the RP-set. Currently, no other router is the preferred BSR, but this router is not yet the elected BSR.

◆ Elected BSR – Elected to serve as BSR.

### WEB INTERFACE

To display information about the BSR:

1. Click Multicast, Multicast Routing, SM.

2. Select Show Information from the Step list.

3. Select Show BSR Router from the Action list.

**Figure 14: Showing Information About the BSR**


## Displaying RP Mapping

Use the Routing Protocol > PIM > SM (Show Information – Show RP Mapping) page to display active RPs and associated multicast routing entries.

### CLI REFERENCES

■"show ip pim rp mapping" on page 1228

### PARAMETERS

These parameters are displayed in the web interface:

■**Groups** – A multicast group address.

■**RP Address** – IP address of the RP for the listed multicast group.

■**Information Source** – RP that advertised the mapping, how the RP was selected (Static or Bootstrap), and the priority used in the bidding process.

■**Uptime** – The time this RP has been up and running

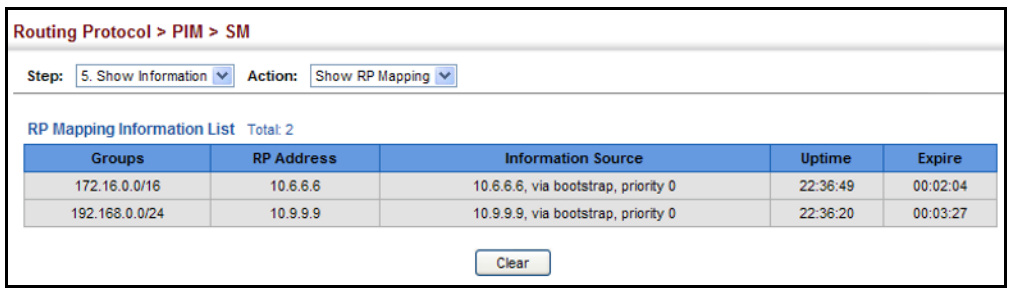
■**Expire** – The time before this entry will be removed.

#### WEB INTERFACE

To display the RPs mapped to multicast groups:

1. Click Multicast, Multicast Routing, SM.
2. Select Show Information from the Step list.
3. Select Show RP Mapping from the Action list.

**Figure 15: Showing RP Mapping**




## CONFIGURING PIMV6 FOR IPV6

This section describes how to configure PIM-DM for IPv6.

### Enabling PIM Globally

Use the Routing Protocol > PIM6 > General page to enable IPv6 PIM routing globally on the router.

#### CLI REFERENCES

■"router pim6" on page 1230

#### COMMAND USAGE

■This feature enables PIM-DM for IPv6 globally on the router. You also need to enable PIM-DM for each interface that will support multicast routing (see page 588), and make any changes necessary to the multicast protocol parameters.

■To use PIMv6, multicast routing must be enabled on the switch (see "Enabling Multicast Routing Globally" on page 568).

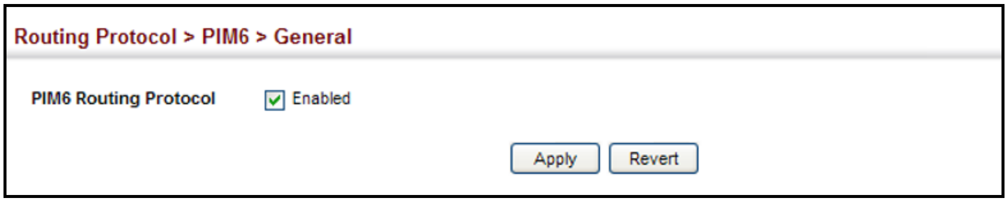
■To use multicast routing, MLD proxy can not enabled on any interface of the device (see "MLD Proxy Routing" on page 1010).

### WEB INTERFACE

To enable PIMv6 multicast routing:

1. Click Routing Protocol, PIM6, General.
2. Enable PIM6 Routing Protocol.
3. Click Apply.

**Figure 16: Enabling PIMv6 Multicast Routing**




## Configuring PIM Interface Settings

Use the Routing Protocol > PIM6 > Interface page configure the routing protocol's functional attributes for each interface.

### CLI REFERENCES

- "IPv6 PIM Commands" on page 1230

### COMMAND USAGE

- PIM-DM functions similar to DVMRP by periodically flooding the network with traffic from any active multicast server. It also uses MLD to determine the presence of multicast group members. The main difference, is that it uses the router's unicast routing table to determine if the interface through which a packet is received provides the shortest path back to the source.

- Dense-mode interfaces are subject to multicast flooding by default, and are only removed from the multicast routing table when the router determines that there are no group members or downstream routers, or when a prune message is received from a downstream router.

- PIMv6 and MLD proxy cannot be used at the same time. When an interface is set to use PIMv6 Dense mode, MLD proxy cannot be enabled on any interface of the device (see "MLD Proxy Routing" on page 1010). Also, when MLD proxy is enabled on an interface, PIMv6 cannot be enabled on any interface.

### PARAMETERS

These parameters are displayed in the web interface:

- **VLAN** – Layer 3 VLAN interface. (Range: 1-4093)

- **Mode** – PIMv6 routing mode. (Options: Dense, None)

- **IPv6 Address** – IPv6 link-local address assigned to the selected VLAN.

- **Hello Holdtime** – Sets the interval to wait for hello messages from a neighboring PIM router before declaring it dead. Note that the hello holdtime should be greater than or equal to the value of Hello Interval, otherwise it will be automatically set to 3.5 x the Hello Interval. (Range: 1-65535 seconds; Default: 105 seconds, or 3.5 times the hello interval if set)

- **Hello Interval** – Sets the frequency at which PIM hello messages are transmitted out on all interfaces. (Range: 1-65535 seconds; Default: 30 seconds)

  Hello messages are sent to neighboring PIM routers from which this device has received probes, and are used to verify whether or not these neighbors are still active members of the multicast tree. PIM-SM routers use these messages not only to inform neighboring routers of their presence, but also to determine which router for each LAN segment will serve as the Designated Router (DR).

  When a router is booted or first configured to use PIM, it sends an initial hello message, and then sets its Hello timer to the configured value. If a router does not hear from a neighbor for the period specified by the Hello Holdtime, that neighbor is dropped. This hold time is included in each hello message received from a neighbor. Also note that hello messages also contain the DR priority of the router sending the message.

  If the hello holdtime is already configured, and the hello interval is set to a value longer than the hello holdtime, this command will fail.

- **Join/Prune Holdtime** – Sets the hold time for the prune state. (Range: 1-65535 seconds; Default: 210 seconds)

  - PIM-DM: The multicast interface that first receives a multicast stream from a particular source forwards this traffic to all other PIM-DM interfaces on the router. If there are no requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The prune state is maintained until the join/prune holdtime timer expires or a graft message is received for the forwarding entry.

  - PIM-SM: The multicast interface that first receives a multicast stream from a particular source forwards this traffic only to those interfaces on the router that have requests to join this group. When there are no longer any requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The protocol maintains both the current join state and the pending RPT prune state for this (source, group) pair until the join/prune interval timer expires.

- **LAN Prune Delay** – Causes this device to inform downstream routers of how long it will wait before pruning a flow after receiving a prune request. (Default: Disabled)

  When other downstream routers on the same VLAN are notified that this upstream router has received a prune request, they must send a Join to override the prune before the prune delay expires if they want to continue receiving the flow. The message generated by this command effectively prompts any downstream neighbors with hosts receiving the flow to reply with a Join message. If no join messages are received after the prune delay expires, this router will prune the flow.

  The sum of the Override Interval and Propagation Delay are used to calculate the LAN prune delay.

- **Override Interval** – The time required for a downstream router to respond to a LAN Prune Delay message by sending back a Join message if it wants to continue receiving the flow referenced in the message. (Range: 500-6000 milliseconds; Default: 2500 milliseconds)

The override interval and the propagation delay are used to calculate the LAN prune delay. If a downstream router has group members which want to continue receiving the flow referenced in a LAN prune delay message, then the override interval represents the time required for the downstream router to process the message and then respond by sending a Join message back to the upstream router to ensure that the flow is not terminated.

- **Propagation Delay** – The time required for a LAN prune delay message to reach downstream routers. (Range: 100-5000 milliseconds; Default: 500 milliseconds)

  The override interval and pro po gat ion delay are used to calculate the LAN prune delay. If a downstream router has group members which want to continue receiving the flow referenced in a LAN prune delay message, then the propagation delay represents the time required for the LAN prune delay message to be propagated down from the upstream router to all downstream routers attached to the same VLAN interface.

- **Trigger Hello Delay** – The maximum time before transmitting a triggered PIM Hello message after the router is rebooted or PIM is enabled on an interface. (Range: 0-5 seconds; Default: 5 seconds)

  When a router first starts or PIM is enabled on an interface, the hello delay is set to random value between 0 and the trigger hello delay. This prevents synchronization of Hello messages on multi-access links if multiple routers are powered on simultaneously.

  Also, if a Hello message is received from a new neighbor, the receiving router will send its own Hello message after a random delay between 0 and the trigger hello delay.

- **Graft Retry Interval** – The time to wait for a Graft acknowledgement before resending a Graft message. (Range: 1-10 seconds; Default: 3 seconds)

  A graft message is sent by a router to cancel a prune state. When a router receives a graft message, it must respond with an graft acknowledgement message. If this acknowledgement message is lost, the router that sent the graft message will resend it a number of times (as defined by Max. Graft Retries).

- **Max. Graft Retries** – The maximum number of times to resend a Graft message if it has not been acknowledged. (Range: 1-10; Default: 3)

- **State Refresh Origination Interval** – The interval between sending PIM-DM state refresh control messages. (Range: 1-100 seconds; Default: 60 seconds)

  The pruned state times out approximately every three minutes and the entire PIM-DM network is reflooded with multicast packets and prune messages. The state refresh feature keeps the pruned state from timing out by periodically forwarding a control message down the distribution tree, refreshing the prune state on the outgoing interfaces of each router in the tree. This also enables PIM routers to recognize topology changes (sources joining or leaving a multicast group) before the default three-minute state timeout expires.

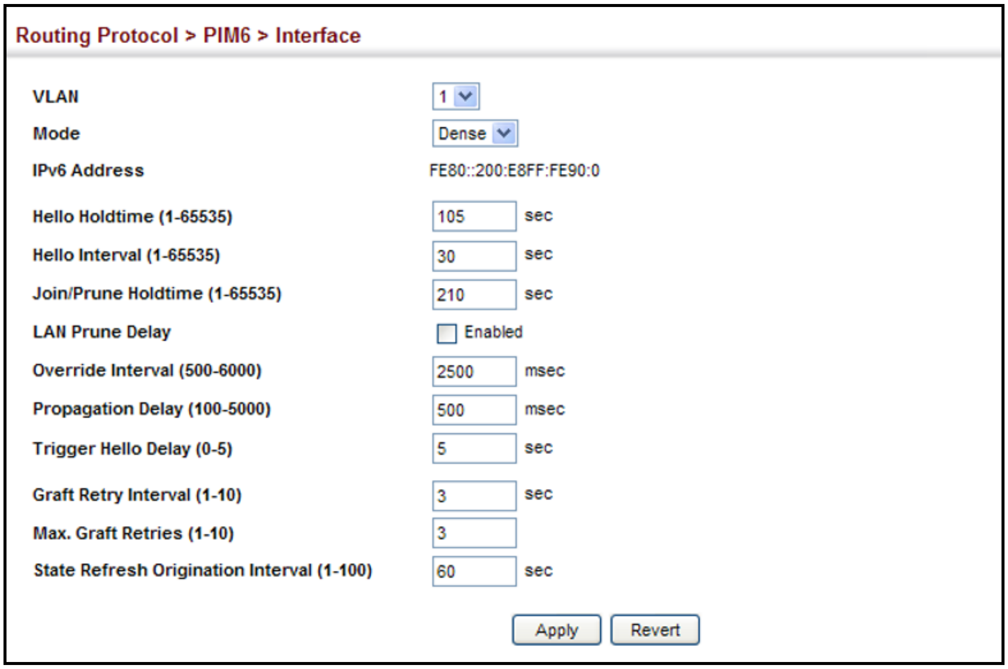
  This command is only effectively for interfaces of first hop, PIM-DM routers that are directly connected to the sources of multicast groups.

### WEB INTERFACE

To configure PIMv6 interface settings:

1. Click Routing Protocol, PIM6, Interface.
2. Modify any of the protocol parameters as required.
3. Click Apply.

**Figure 17: Configuring PIMv6 Interface Settings** (Dense Mode)




## Displaying Neighbor Information

Use the Routing Protocol > PIM6 > Neighbor page to display all neighboring PIMv6 routers.

### CLI REFERENCES

- "show ip pim neighbor" on page 1216

### PARAMETERS

These parameters are displayed in the web interface:

- **Address** – IP address of the next-hop router.
- **VLAN** – VLAN that is attached to this neighbor.
- **Uptime** – The duration this entry has been active.
- **Expire** – The time before this entry will be removed.

### WEB INTERFACE

To display neighboring PIMv6 routers:

1. Click Routing Protocol, PIM6, Neighbor.

**Figure 18: Showing PIMv6 Neighbors**

Routing Protocol > PIM6 > Neighbor

Neighbor Information Max: 128 Total: 2

| Address | VLAN | Uptime | Expire |
|---|---|---|---|
| 10.1.2.50 | 1 | 00:01:23 | 00:01:23 |
| 10.1.2.51 | 2 | 1d11h | Never |

# COMMAND LINE INTERFACE

This section provides a detailed description of the Command Line Interface, along with examples for all of the commands.

This section includes these chapters:

# 23 USING THE COMMAND LINE INTERFACE

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

## ACCESSING THE CLI

When accessing the management interface for the switch over a direct connection to the server's console port, or via a Telnet or Secure Shell connection (SSH), the switch can be managed by entering command keywords and parameters at the prompt. Using the switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

### CONSOLE CONNECTION

To access the switch through the console port, perform these steps:

1. At the console prompt, enter the user name and password. (The default user names are "admin" and "guest" with corresponding passwords of "admin" and "guest.") When the administrator user name and password is entered, the CLI displays the "Console#" prompt and enters privileged access mode (i.e., Privileged Exec). But when the guest user name and password is entered, the CLI displays the "Console>" prompt and enters normal access mode (i.e., Normal Exec).

2. Enter the necessary commands to complete your desired tasks.

3. When finished, exit the session with the "quit" or "exit" command.

After connecting to the system through the console port, the login screen displays:

```
User Access Verification
Username: admin
Password:
  CLI session with the EL326 is opened.
  To end the CLI session, enter [Exit].
Console#
```

## TELNET CONNECTION

Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion. For example, the IP address assigned to this switch, 10.1.0.1, consists of a network portion (10.1.0) and a host portion (1).

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

To access the switch through a Telnet session, you must first set the IP address for the Master unit, and set the default gateway if you are managing the switch from a different IP subnet. For example,

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.254 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
Console(config)#
```

If your corporate network is connected to another network outside your office or to the Internet, you need to apply for a registered IP address. However, if you are attached to an isolated network, then you can use any IP address that matches the network segment to which you are attached.

After you configure the switch with an IP address, you can open a Telnet session by performing these steps:

1. From the remote host, enter the Telnet command and the IP address of the device you want to access.
2. At the prompt, enter the user name and system password. The CLI will display the "Vty-*n*#" prompt for the administrator to show that you are using privileged access mode (i.e., Privileged Exec), or "Vty-*n*>" for the guest to show that you are using normal access mode (i.e., Normal Exec), where *n* indicates the number of the current Telnet session.
3. Enter the necessary commands to complete your desired tasks.
4. When finished, exit the session with the "quit" or "exit" command.

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:

 CLI session with the EL326T is opened.
 To end the CLI session, enter [Exit].

Vty-0#
```

**NOTE:** You can open up to four sessions to the device via Telnet or SSH.

## ENTERING COMMANDS

This section describes how to enter CLI commands.

### KEYWORDS AND ARGUMENTS

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command “show interfaces status ethernet 1/5,” **show interfaces** and **status** are keywords, **ethernet** is an argument that specifies the interface type, and **1/5** specifies the unit/port.

You can enter commands as follows:

- To enter a simple command, enter the command keyword.
- To enter multiple commands, enter each command in the required order. For example, to enable Privileged Exec command mode, and display the startup configuration, enter:

  Console>**enable**
  Console#**show startup-config**

- To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

  Console(config)#**username admin password 0 smith**

### MINIMUM ABBREVIATION

The CLI will accept a minimum number of characters that uniquely identify a command. For example, the command “configure” can be entered as **con**. If an entry is ambiguous, the system will prompt for further input.

### COMMAND COMPLETION

If you terminate input with a Tab key, the CLI will print the remaining characters of a partial keyword up to the point of ambiguity. In the “logging history” example, typing **log** followed by a tab will result in printing the command up to “**logging**.”

## GETTING HELP ON COMMANDS

You can display a brief description of the help system by entering the **help** command. You can also display command syntax by using the “?” character to list keywords or parameters.

### SHOWING COMMANDS

If you enter a “?” at the command prompt, the system will display the first level of keywords or command groups. You can also display a list of valid keywords for a specific command. For example, the command “**show ?**” displays a list of possible show commands:

```
Console#show ?
  access-group         Access groups
  access-list          Access lists
  accounting           Uses the specified accounting list
  arp                  Information of ARP cache
  authorization        Authorization configurations
  auto-traffic-control Auto traffic control information
  bridge-ext           Bridge extension information
  cable-diagnostics    Shows the information of cable diagnostics
  calendar             Date and time information
  class-map            Displays class maps
  dns                  DNS information
  dot1q-tunnel         802.1Q tunnel
  dot1x                802.1X content
  garp                 GARP properties
  gvrp                 GVRP interface information
  history              Shows history information
  hosts                Host information
  interfaces           Shows interface information
  ip                   IP information
  ipv6                 IPv6 information
  lacp                 LACP statistics
  line                 TTY line information
  lldp                 LLDP
  log                  Log records
  logging              Logging setting
  loop                 Shows the information of loopback
  mac                  MAC access list
  mac-address-table    Configuration of the address table
  mac-vlan             MAC-based VLAN information
  management           Shows management information
  map                  Maps priority
  memory               Memory utilization
  mvr                  Multicast VLAN registration
  network-access       Shows the entries of the secure port
  nlm                  Show notification log
  policy-map           Displays policy maps
  port                 Port characteristics
  process              Device process
  protocol-vlan        Protocol-VLAN information
  public-key           Public key information
  queue                Priority queue information
  radius-server        RADIUS server information
  reload               Shows the reload settings
  rmon                 Remote Monitoring Protocol
  running-config       Information on the running configuration
  sflow                Shows the sflow information
  snmp                 Simple Network Management Protocol configuration and
                       statistics
  sntp                 Simple Network Time Protocol configuration
  spanning-tree        Spanning-tree configuration
```

```
  ssh                Secure shell server connections
  startup-config     Startup system configuration
  subnet-vlan        IP subnet-based VLAN information
  system             System information
  tacacs-server      TACACS server information
  tech-support       Technical information
  time-range         Time range
  traffic-segmentation  Traffic segmentation information
  users              Information about users logged in
  version            System hardware and software versions
  vlan               Shows virtual LAN settings
  voice              Shows the voice VLAN information
  vrrp               Shows VRRP
  web-auth           Shows web authentication configuration
Console#show
```

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

```
Console#show interfaces ?
  brief          brief interface description
  counters       Interface counters information
  protocol-vlan  Protocol-VLAN information
  status         Shows interface status
  switchport     Shows interface switchport information
  transceiver    Interface of transceiver information
Console#
```

Show commands which display more than one page of information (e.g., **show running-config**) pause and require you to press the [Space] bar to continue displaying one more page, the [Enter] key to display one more line, or the [a] key to display the rest of the information without stopping. You can press any other key to terminate the display.

### PARTIAL KEYWORD LOOKUP

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and question mark.) For example "**s?**" shows all the keywords starting with "s."

```
Console#show s?
sflow          snmp          sntp          spanning-tree   ssh
startup-config  subnet-vlan     system
Console#show s
```

### NEGATING THE EFFECT OF COMMANDS

For many configuration commands you can enter the prefix keyword "**no**" to cancel the effect of a command or reset the configuration to the default value. For example, the **logging** command will log system messages to a host server. To disable logging, specify the **no logging** command. This guide describes the negation effect for all applicable commands.

## USING COMMAND HISTORY

The CLI maintains a history of commands that have been entered. You can scroll back through the history of commands by pressing the up arrow key. Any command displayed in the history list can be executed again, or first modified and then executed.

Using the **show history** command displays a longer list of recently executed commands.

## UNDERSTANDING COMMAND MODES

The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain switching functions. These classes are further divided into different modes. Available commands depend on the selected mode. You can always enter a question mark "**?**" at the prompt to display a list of the commands available for the current mode. The command classes and associated modes are displayed in the following table:

**Table 1: General Command Modes**

| Class | Mode | |
|---|---|---|
| Exec | Normal<br>Privileged | |
| Configuration | Global[1] | Access Control List<br>Class Map<br>DHCP<br>IGMP Profile<br>Interface<br>Line<br>Multiple Spanning Tree<br>Policy Map<br>Router<br>Time Range<br>VLAN Database |

1. You must be in Privileged Exec mode to access the Global configuration mode.
   You must be in Global Configuration mode to access any of the other configuration modes.

## EXEC COMMANDS

When you open a new console session on the switch with the user name and password "guest," the system enters the Normal Exec command mode (or guest mode), displaying the "Console>" command prompt. Only a limited number of the commands are available in this mode. You can access all commands only from the Privileged Exec command mode (or administrator mode). To access Privilege Exec mode, open a new console session with the user name and password "admin." The system will now display the "Console#" command prompt. You can also enter Privileged Exec mode from within Normal Exec mode, by entering the enable command, followed by the privileged level password "super."

To enter Privileged Exec mode, enter the following user names and passwords:

```
Username: admin
Password: [admin login password]

  CLI session with the EL326 is opened.
  To end the CLI session, enter [Exit].

Console#
```

```
Username: guest
Password: [guest login password]

  CLI session with the EL326 is opened.
  To end the CLI session, enter [Exit].

Console>enable
Password: [privileged level password]
Console#
```

## CONFIGURATION COMMANDS

Configuration commands are privileged level commands used to modify switch settings. These commands modify the running configuration only and are not saved when the switch is rebooted. To store the running configuration in non-volatile storage, use the **copy running-config startup-config** command.

The configuration commands are organized into different modes:

- 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.
- Class Map Configuration - Creates a DiffServ class map for a specified traffic type.
- DHCP Configuration - These commands are used to configure the DHCP server.
- IGMP Profile - Sets a profile group and enters IGMP filter profile configuration mode.
- Interface Configuration - These commands modify the port configuration such as **speed-duplex** and **negotiation**.
- Line Configuration - These commands modify the console port and Telnet configuration, and include command such as **parity** and **databits**.
- Multiple Spanning Tree Configuration - These commands configure settings for the selected multiple spanning tree instance.
- Policy Map Configuration - Creates a DiffServ policy map for multiple interfaces.
- Router Configuration - These commands configure global settings for unicast and multicast routing protocols.

- Time Range - Sets a time range for use by other functions, such as Access Control Lists.
- VLAN Configuration - Includes the command to create VLAN groups.

To enter the Global Configuration mode, enter the command **configure** in Privileged Exec mode. The system prompt will change to "Console(config)#" which gives you access privilege to all Global Configuration commands.

```
Console#configure
Console(config)#
```

To enter the other modes, at the configuration prompt type one of the following commands. Use the **exit** or **end** command to return to the Privileged Exec mode.

**Table 2: Configuration Command Modes**

| Mode | Command | Prompt | Page |
|---|---|---|---|
| Access Control List | access-list arp<br>access-list ip standard<br>access-list ip extended<br>access-list mac<br>access-list ipv6 standard<br>access-list ipv6 extended | Console(config-arp-acl)<br>Console(config-std-acl)<br>Console(config-ext-acl)<br>Console(config-mac-acl)<br>Console(config-std-ipv6-acl)<br>Console(config-ext-ipv6-acl) | 801<br>784<br>784<br>796<br>791<br>792 |
| Class Map | class-map | Console(config-cmap) | 942 |
| DHCP | ip dhcp pool | Console(config-dhcp) | 1044 |
| Line | line {console \| vty} | Console(config-line) | 631 |
| Interface | interface {ethernet *port* \| port-channel *id*\| vlan *id*} | Console(config-if) | 806 |
| MSTP | spanning-tree mst-configuration | Console(config-mstp) | 865 |
| Policy Map | policy-map | Console(config-pmap) | 945 |
| Router | router<br>{ipv6 ospf \| pim \| pim6 \| rip \| ospf} | Console(config-router) | 1177<br>1209<br>1230<br>1121<br>1139 |
| Time Range | time-range | Console(config-time-range) | 654 |
| VLAN | vlan database | Console(config-vlan) | 891 |

For example, you can use the following commands to enter interface configuration mode, and then return to Privileged Exec mode

```
Console(config)#interface ethernet 1/5
.
.
.
Console(config-if)#exit
Console(config)#
```

## COMMAND LINE PROCESSING

Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the “?” character to display a list of possible matches. You can also use the following editing keystrokes for command-line processing:

**Table 3: Keystroke Commands**

| Keystroke | Function |
|---|---|
| Ctrl-A | Shifts cursor to start of command line. |
| Ctrl-B | Shifts cursor to the left one character. |
| Ctrl-C | Terminates the current task and displays the command prompt. |
| Ctrl-E | Shifts cursor to end of command line. |
| Ctrl-F | Shifts cursor to the right one character. |
| Ctrl-K | Deletes all characters from the cursor to the end of the line. |
| Ctrl-L | Repeats current command line on a new line. |
| Ctrl-N | Enters the next command line in the history buffer. |
| Ctrl-P | Enters the last command. |
| Ctrl-R | Repeats current command line on a new line. |
| Ctrl-U | Deletes from the cursor to the beginning of the line. |
| Ctrl-W | Deletes the last word typed. |
| Esc-B | Moves the cursor back one word. |
| Esc-D | Deletes from the cursor to the end of the word. |
| Esc-F | Moves the cursor forward one word. |
| Delete key or backspace key | Erases a mistake when entering a command. |

## CLI COMMAND GROUPS

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

**Table 4: Command Group Index**

| Command Group | Description | Page |
|---|---|---|
| General | Basic commands for entering privileged access mode, restarting the system, or quitting the CLI | 607 |
| System Management | Display and setting of system information, basic modes of operation, maximum frame size, file management, console port and telnet settings, system logs, SMTP alerts, and the system clock | 615 |
| Simple Network Management Protocol | Activates authentication failure traps; configures community access strings, and trap receivers | 659 |
| Remote Monitoring | Supports statistics, history, alarm and event groups | 677 |
| Flow Sampling | Samples traffic flows, and forwards data to designated collector | 685 |
| User Authentication | Configures user names and passwords, logon access using local or remote authentication, management access through the web server, Telnet server and Secure Shell; as well as port security, IEEE 802.1X port access control, and restricted access based on specified IP addresses | 691 |
| General Security Measures | Segregates traffic for clients attached to common data ports; and prevents unauthorized access by configuring valid static or dynamic addresses, web authentication, MAC address authentication, filtering DHCP requests and replies, and discarding invalid ARP responses | 739 |
| Access Control List | Provides filtering for IPv4 frames (based on address, protocol, TCP/UDP port number or TCP control code), IPv6 frames (based on address, DSCP traffic class, next header, or flow label), or non-IP frames (based on MAC address or Ethernet type) | 783 |
| Interface | Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs | 805 |
| Link Aggregation | Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks | 823 |
| Mirror Port | Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port | 833 |
| Rate Limit | Controls the maximum rate for traffic transmitted or received on a port | 837 |
| Automatic Traffic Control | Configures bounding thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port | 839 |
| Address Table | Configures the address table for filtering specified addresses, displays current entries, clears the table, or sets the aging time | 853 |
| Spanning Tree | Configures Spanning Tree settings for the switch | 859 |
| VLANs | Configures VLAN settings, and defines port membership for VLAN groups; also enables or configures private VLANs, protocol VLANs, voice VLANs, and QinQ tunneling | 885 |
| Class of Service | Sets port priority for untagged frames, selects strict priority or weighted round robin, relative weight for each priority queue, also sets priority for TCP/UDP traffic types, IP precedence, and DSCP | 927 |
| Quality of Service | Configures Differentiated Services | 941 |

**Table 4: Command Group Index (Continued)**

| Command Group | Description | Page |
|---|---|---|
| Multicast Filtering | Configures IGMP multicast filtering, query, profile, and proxy parameters; specifies ports attached to a multicast router; also configures multicast VLAN registration | 957 |
| Link Layer Discovery Protocol | Configures LLDP settings to enable information discovery about neighbor devices | 1013 |
| Domain Name Service | Configures DNS services. | 1031 |
| Dynamic Host Configuration Protocol | Configures DHCP client, relay and server functions | 1039 |
| Router Redundancy | Configures router redundancy to create primary and backup routers | 1057 |
| IP Interface | Configures IP address for the switch interfaces; also configures ARP parameters and static entries | 1067 |
| IP Routing | Configures static and dynamic unicast routing | 1113 |
| Multicast Routing | Configures multicast routing protocols PIM-DM and PIM-SM | 1201 |

The access mode shown in the following tables is indicated by these abbreviations:

**ACL** (Access Control List Configuration)
**CM** (Class Map Configuration)
**DC** (DHCP Server Configuration)
**GC** (Global Configuration)
**IC** (Interface Configuration)
**IPC** (IGMP Profile Configuration)
**LC** (Line Configuration)
**MST** (Multiple Spanning Tree)
**NE** (Normal Exec)
**PE** (Privileged Exec)
**PM** (Policy Map Configuration)
**RC** (Router Configuration)
**VC** (VLAN Database Configuration)

# 24 GENERAL COMMANDS

These commands are used to control the command access mode, configuration mode, and other basic functions.

**Table 1: General Commands**

| Command | Function | Mode |
|---|---|---|
| prompt | Customizes the CLI prompt | GC |
| reload | Restarts the system at a specified time, after a specified delay, or at a periodic interval | GC |
| enable | Activates privileged mode | NE |
| quit | Exits a CLI session | NE, PE |
| show history | Shows the command history buffer | NE, PE |
| configure | Activates global configuration mode | PE |
| disable | Returns to normal mode from privileged mode | PE |
| reload | Restarts the system immediately | PE |
| show reload | Displays the current reload settings, and the time at which next scheduled reload will take place | PE |
| end | Returns to Privileged Exec mode | any config. mode |
| exit | Returns to the previous configuration mode, or exits the CLI | any mode |
| help | Shows how to use help | any mode |
| ? | Shows options for command completion (context sensitive) | any mode |

## prompt

This command customizes the CLI prompt. Use the **no** form to restore the default prompt.

### SYNTAX

**prompt** *string*

**no prompt**

*string* - Any alphanumeric string to use for the CLI prompt. (Maximum length: 255 characters)

### DEFAULT SETTING

Console

### COMMAND MODE

Global Configuration

### EXAMPLE

```
Console(config)#prompt RD2
RD2(config)#
```

## reload (Global Configuration)

This command restarts the system at a specified time, after a specified delay, or at a periodic interval. You can reboot the system immediately, or you can configure the switch to reset after a specified amount of time. Use the **cancel** option to remove a configured setting.

### SYNTAX

**reload** {**at** *hour minute* [{*month day* | *day month*} [*year*]] |
**in** {**hour** *hours* | **minute** *minutes* | **hour** *hours* **minute** *minutes*} |
**regularity** *hour minute* [**period** {**daily** | **weekly** *day-of-week* | **monthly** *day*}] |
**cancel** [**at** | **in** | **regularity**]}

**reload at** - A specified time at which to reload the switch.

*hour* - The hour at which to reload. (Range: 0-23)

*minute* - The minute at which to reload. (Range: 0-59)

*month* - The month at which to reload. (january ... december)

*day* - The day of the month at which to reload. (Range: 1-31)

*year* - The year at which to reload. (Range: 2001-2050)

**reload in** - An interval after which to reload the switch.

*hours* - The number of hours, combined with the minutes, before the switch resets. (Range: 0-576)

*minutes* - The number of minutes, combined with the hours, before the switch resets. (Range: 0-59)

**reload regularity** - A periodic interval at which to reload the switch.

*hour* - The hour at which to reload. (Range: 0-23)

*minute* - The minute at which to reload. (Range: 0-59)

day-of-week - Day of the week at which to reload.
(Range: monday ... saturday)

*day* - Day of the month at which to reload. (Range: 1-31)

**reload cancel** - Cancels the specified reload option.

### DEFAULT SETTING

None

### COMMAND MODE

Global Configuration

#### COMMAND USAGE

- This command resets the entire system.
- Any combination of reload options may be specified. If the same option is re-specified, the previous setting will be overwritten.
- When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory by the copy running-config startup-config command (See "copy" on page 625).

#### EXAMPLE

This example shows how to reset the switch after 30 minutes:

```
Console(config)#reload in minute 30
***
*** --- Rebooting at January  1 02:10:43 2007 ---
***

Are you sure to reboot the system at the specified time? <y/n>
```

## enable

This command activates Privileged Exec mode. In privileged mode, additional commands are available, and certain commands display additional information. See "Understanding Command Modes" on page 604.

#### SYNTAX

**enable** [*level*]

*level* - Privilege level to log into the device.

The device has two predefined privilege levels: 0: Normal Exec, 15: Privileged Exec. Enter level 15 to access Privileged Exec mode.

#### DEFAULT SETTING

Level 15

#### COMMAND MODE

Normal Exec

#### COMMAND USAGE

- “super” is the default password required to change the command mode from Normal Exec to Privileged Exec. (To set this password, see the enable password command.)
- The “#” character is appended to the end of the prompt to indicate that the system is in privileged access mode.

#### EXAMPLE

```
Console>enable
Password: [privileged level password]
Console#
```

#### RELATED COMMANDS
disable (611)
enable password (692)

### quit
This command exits the configuration program.

#### DEFAULT SETTING
None

#### COMMAND MODE
Normal Exec, Privileged Exec

#### COMMAND USAGE
The **quit** and **exit** commands can both exit the configuration program.

#### EXAMPLE
This example shows how to quit a CLI session:

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```

### show history
This command shows the contents of the command history buffer.

#### DEFAULT SETTING
None

#### COMMAND MODE
Normal Exec, Privileged Exec

#### COMMAND USAGE
The history buffer size is fixed at 10 Execution commands and 10 Configuration commands.

#### EXAMPLE
In this example, the show history command lists the contents of the command history buffer:

```
Console#show history
Execution command history:
 2 config
 1 show history

Configuration command history:
 4 interface vlan 1
```

```
3 exit
2 interface vlan 1
1 end

Console#
```

The **!** command repeats commands from the Execution command history buffer when you are in Normal Exec or Privileged Exec Mode, and commands from the Configuration command history buffer when you are in any of the configuration modes. In this example, the **!2** command repeats the second command in the Execution history buffer (**config**).

```
Console#!2
Console#config
Console(config)#
```

## configure

This command activates Global Configuration mode. You must enter this mode to modify any settings on the switch. You must also enter Global Configuration mode prior to enabling some of the other configuration modes, such as Interface Configuration, Line Configuration, and VLAN Database Configuration. See "Understanding Command Modes" on page 604.

### DEFAULT SETTING

None

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#configure
Console(config)#
```

### RELATED COMMANDS

end (613)

## disable

This command returns to Normal Exec mode from privileged mode. In normal access mode, you can only display basic information on the switch's configuration or Ethernet statistics. To gain access to all commands, you must use the privileged mode. See "Understanding Command Modes" on page 604.

### DEFAULT SETTING

None

### COMMAND MODE

Privileged Exec

#### COMMAND USAGE

The “>” character is appended to the end of the prompt to indicate that the system is in normal access mode.

#### EXAMPLE

```
Console#disable
Console>
```

#### RELATED COMMANDS

enable (609)

### reload (Privileged Exec)

This command restarts the system.

**NOTE:** When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory by the copy running-config startup-config command.

#### DEFAULT SETTING

None

#### COMMAND MODE

Privileged Exec

#### COMMAND USAGE

This command resets the entire system.

#### EXAMPLE

This example shows how to reset the switch:

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

### show reload

This command displays the current reload settings, and the time at which next scheduled reload will take place.

#### COMMAND MODE

Privileged Exec

#### EXAMPLE

```
Console#show reload
Reloading switch in time:                0 hours 29 minutes.

The switch will be rebooted at January  1 02:11:50 2001.
```

```
Remaining Time: 0 days, 0 hours, 29 minutes, 52 seconds.
Console#
```

## end

This command returns to Privileged Exec mode.

**DEFAULT SETTING**
None

**COMMAND MODE**
Global Configuration, Interface Configuration, Line Configuration, VLAN Database Configuration, and Multiple Spanning Tree Configuration.

**EXAMPLE**
This example shows how to return to the Privileged Exec mode from the Interface Configuration mode:

```
Console(config-if)#end
Console#
```

## exit

This command returns to the previous configuration mode or exits the configuration program.

**DEFAULT SETTING**
None

**COMMAND MODE**
Any

**EXAMPLE**
This example shows how to return to the Privileged Exec mode from the Global Configuration mode, and then quit the CLI session:

```
Console(config)#exit
Console#exit

Press ENTER to start session

User Access Verification

Username:
```

# 25 SYSTEM MANAGEMENT COMMANDS

These commands are used to control system logs, passwords, user names, management options, and display or configure a variety of other system information.

**Table 1: System Management Commands**

| Command Group | Function |
|---|---|
| Device Designation | Configures information that uniquely identifies this switch |
| System Status | Displays system configuration, active managers, and version information |
| Fan Control | Forces fans to full speed |
| Frame Size | Enables support for jumbo frames |
| File Management | Manages code image or switch configuration files |
| Line | Sets communication parameters for the serial port, including baud rate and console time-out |
| Event Logging | Controls logging of error messages |
| SMTP Alerts | Configures SMTP email alerts |
| Time (System Clock) | Sets the system clock automatically via NTP/SNTP server or manually |
| Time Range | Sets a time range for use by other functions, such as Access Control Lists |

## DEVICE DESIGNATION

This section describes commands used to configure information that uniquely identifies the switch.

**Table 2: Device Designation Commands**

| Command | Function | Mode |
|---|---|---|
| hostname | Specifies the host name for the switch | GC |
| snmp-server contact | Sets the system contact string | GC |
| snmp-server location | Sets the system location string | GC |

### hostname

This command specifies or modifies the host name for this device. Use the **no** form to restore the default host name.

#### SYNTAX

**hostname** *name*

**no hostname**

*name* - The name of this host. (Maximum length: 255 characters)

### DEFAULT SETTING

None

### COMMAND MODE

Global Configuration

### EXAMPLE

```
Console(config)#hostname RD#1
Console(config)#
```

## SYSTEM STATUS

This section describes commands used to display system information.

**Table 3: System Status Commands**

| Command | Function | Mode |
|---|---|---|
| show access-list tcam-utilization | Shows utilization parameters for TCAM | PE |
| show memory | Shows memory utilization parameters | NE, PE |
| show process cpu | Shows CPU utilization parameters | NE, PE |
| show running-config | Displays the configuration data currently in use | PE |
| show startup-config | Displays the contents of the configuration file (stored in flash memory) that is used to start up the system | PE |
| show system | Displays system information | NE, PE |
| show tech-support | Displays a detailed list of system settings designed to help technical support resolve configuration or functional problems | PE |
| show users | Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet clients | NE, PE |
| show version | Displays version information for the system | NE, PE |

### show access-list tcam-utilization

This command shows utilization parameters for TCAM (Ternary Content Addressable Memory), including the number policy control entries in use, the number of free entries, and the overall percentage of TCAM in use.

### COMMAND MODE

Privileged Exec

### COMMAND USAGE

Policy control entries (PCEs) are used by various system functions which rely on rule-based searches, including Access Control Lists (ACLs), IP Source Guard filter rules, Quality of Service (QoS) processes, or traps.

For example, when binding an ACL to a port, each rule in an ACL will use two PCEs; and when setting an IP Source Guard filter rule for a port, the system will also use two PCEs.

#### EXAMPLE

```
Console#show access-list tcam-utilization
  Total Policy Control Entries : 512
  Free Policy Control Entries  : 508
  TCAM Utilization             : 0.78%
Console#
```

### show memory

This command shows memory utilization parameters.

#### COMMAND MODE

Normal Exec, Privileged Exec

#### COMMAND USAGE

This command shows the amount of memory currently free for use, the amount of memory allocated to active processes, and the total amount of system memory.

#### EXAMPLE

```
Console#show memory
 Status   Bytes
 ------ ----------
 Free    134946816
 Used    133488640
Total    268435456

Console#
```

### show process cpu

This command shows the CPU utilization parameters.

#### COMMAND MODE

Normal Exec, Privileged Exec

#### EXAMPLE

```
Console#show process cpu
 CPU Utilization in the past 5 seconds : 3.98%

Console#
```

### show running-config

This command displays the configuration information currently in use.

#### SYNTAX

**show running-config** [**interface** *interface*]

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

**vlan** *vlan-id* (Range: 1-4093)

### Command Mode

Privileged Exec

### Command Usage

- Use the **interface** keyword to display configuration data for the specified interface.
- 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:
  - SNMP community strings
  - Users (names, access levels, and encrypted passwords)
  - VLAN database (VLAN ID, name and state)
  - VLAN configuration settings for each interface
  - Multiple spanning tree instances (name and interfaces)
  - IP address configured for VLANs
  - Layer 4 precedence settings
  - Routing protocol configuration settings
  - Spanning tree settings
  - Interface settings
  - Any configured settings for the console port and Telnet

### Example

```
Console#show running-config
Building running configuration. Please wait...
snmp-server community public ro
snmp-server community private rw
!
snmp-server enable traps authentication
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
!
spanning-tree mst configuration
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
:
!
interface vlan 1
 ip address dhcp
!
no ip igmp snooping proxy-reporting
```

```
!
interface vlan 1
!
line console
!
line vty
!
end
!
Console#show running-config interface ethernet 1/1
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
 queue weight 1 2 4 6 8 10 12 14
!
Console#
```

**RELATED COMMANDS**

show startup-config (619)

## show startup-config

This command displays the configuration file stored in non-volatile memory that is used to start up the system.

**COMMAND MODE**

Privileged Exec

**COMMAND USAGE**

- Use this command in conjunction with the **show running-config** command to compare the information in running memory to the information stored in non-volatile memory.

- This command displays settings for key command modes. Each mode group is separated by "!" symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
  - SNMP community strings
  - Users (names, access levels, and encrypted passwords)
  - VLAN database (VLAN ID, name and state)
  - VLAN configuration settings for each interface
  - Multiple spanning tree instances (name and interfaces)
  - IP address configured for VLANs
  - Layer 4 precedence settings
  - Routing protocol configuration settings
  - Spanning tree settings
  - Interface settings
  - Any configured settings for the console port and Telnet

**EXAMPLE**

Refer to the example for the running configuration file.

**RELATED COMMANDS**

show running-config (617)

## show system

This command displays system information.

### DEFAULT SETTING
None

### COMMAND MODE
Normal Exec, Privileged Exec

### COMMAND USAGE
- For a description of the items shown by this command, refer to "Displaying System Information" on page 85.
- There are two thermal detectors. The first detector is near the air flow intake vents. The second detector is near the switch ASIC.
- No information will be displayed under POST Result, unless there is a problem with the unit. If any POST test indicates "FAIL," contact your distributor for assistance.

### EXAMPLE

```
Console#show system
System Description : EL 326
System OID String  : 1.3.6.1.4.1.259.10.1.1
System Information
 System Up Time       : 0 days, 0 hours, 21 minutes, and 47.6 seconds
 System Name          :
 System Location      :
 System Contact       :
 MAC Address (Unit 1)  : 00-00-E8-93-82-A0
 Web Server           : Enabled
 Web Server Port      : 80
 Web Secure Server     : Enabled
 Web Secure Server Port : 443
 Telnet Server        : Enabled
 Telnet Server Port    : 23
 Jumbo Frame          : Disabled

System Fan:
 Force Fan Speed Full  : Disabled
Unit 1
 Fan 1: Ok               Fan 2: Ok               Fan 3: Ok
System Temperature:
Unit 1
 Temperature 1:  28 degrees     Temperature 2:  44 degrees

Console#
```

## show tech-support

This command displays a detailed list of system settings designed to help technical support resolve configuration or functional problems.

### COMMAND MODE
Normal Exec, Privileged Exec

#### COMMAND USAGE

This command generates a long list of information including detailed system and interface settings. It is therefore advisable to direct the output to a file using any suitable output capture function provided with your terminal emulation program.

#### EXAMPLE

```
Console#show tech-support

show system:
System Description : EL 326
System OID String  : 1.3.6.1.4.1.259.10.1.1
System Information
 System Up Time:         0 days, 2 hours, 17 minutes, and 6.23 seconds
 System Name:            [NONE]
 System Location:        [NONE]
 System Contact:         [NONE]
 MAC Address (Unit1):     00-12-CF-61-24-2F
 Web Server:             Enabled
 Web Server Port:        80
 Web Secure Server:       Enabled
 Web Secure Server Port:  443
 Telnet Server:          Enable
 Telnet Server Port:     23
 Jumbo Frame:            Disabled
:
```

### show users

Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet client.

#### DEFAULT SETTING

None

#### COMMAND MODE

Normal Exec, Privileged Exec

#### COMMAND USAGE

The session used to execute this command is indicated by a “*” symbol next to the Line (i.e., session) index number.

#### EXAMPLE

```
Console#show users
 User Name Accounts:
  User Name Privilege Public-Key
  --------- --------- ----------
     admin        15 None
     guest         0 None
     steve        15  RSA

 Online Users:
  Line    User Name                  Idle time (h:m:s) Remote IP addr
  ------- -------------------------------- ----------------- ---------------
* Console admin                           0:00:00
  SSH 0                               0:05:59 ::FFFF:192.168.0.61
  VTY 2   admin                          0:00:03 192.168.0.61

 Web Online Users:
```

```
Line  User Name                    Idle time (h:m:s) Remote IP Addr
----- ---------------------------- ----------------- ---------------
HTTP  admin                        0:01:24 192.168.0.61

Console#
```

**show version** This command displays hardware and software version information for the system.

### COMMAND MODE

Normal Exec, Privileged Exec

### COMMAND USAGE

See "Displaying Switch Hardware/Software Versions" on page 86 for detailed information on the items displayed by this command.

### EXAMPLE

```
Console#show version
Unit 1
 Serial Number          : S123456
 Hardware Version       : R0A
 EPLD Version           : 1.06
 Number of Ports        : 26
 Main Power Status      : Up
 Redundant Power Status : Not present
 Role                   : Master
 Loader Version         : 1.1.0.1
 Linux Kernel Version   : 2.6.19.2-0.1
 Boot ROM Version       : 0.0.0.1
 Operation Code Version : 1.2.1.2

Console#
```

## FRAME SIZE

This section describes commands used to configure the Ethernet frame size on the switch.

**Table 4: Frame Size Commands**

| Command | Function | Mode |
|---|---|---|
| jumbo frame | Enables support for jumbo frames | GC |

**jumbo frame** This command enables support for jumbo frames for Gigabit Ethernet ports. Use the **no** form to disable it.

### SYNTAX

[**no**] **jumbo frame**

#### DEFAULT SETTING
Disabled

#### COMMAND MODE
Global Configuration

#### COMMAND USAGE
- This switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames on Gigabit Ethernet ports up to 10K bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

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

- The current setting for jumbo frames can be displayed with the show system command.

#### EXAMPLE

```
Console(config)#jumbo frame
Console(config)#
```

#### RELATED COMMANDS
show ipv6 mtu (1091)

## FAN CONTROL

This section describes the command used to force fan speed.

**Table 5: Fan Control Commands**

| Command | Function | Mode |
|---|---|---|
| fan-speed force-full | Forces fans to full speed | GC |
| show system | Shows if full fan speed is enabled | NE, PE |

### fan-speed force-full

This command sets all fans to full speed. Use the no form to reset the fans to normal operating speed.

#### SYNTAX

[**no**] **fan-speed force-full**

#### DEFAULT SETTING
Normal speed

### COMMAND MODE

Global Configuration

### EXAMPLE

```
Console(config)#fan-speed force-full
Console(config)#
```

## FILE MANAGEMENT

**Managing Firmware**

Firmware can be uploaded and downloaded to or from an FTP/TFTP server. By saving runtime code to a file on an FTP/TFTP server, that file can later be downloaded to the switch to restore operation. The switch can also be set to use new firmware without overwriting the previous version.

When downloading runtime code, the destination file name can be specified to replace the current image, or the file can be first downloaded using a different name from the current runtime code file, and then the new file set as the startup file.

**Saving or Restoring Configuration Settings**

Configuration settings can be uploaded and downloaded to and from an FTP/TFTP server. The configuration file can be later downloaded to restore switch settings.

The configuration file can be downloaded under a new file name and then set as the startup file, or the current startup configuration file can be specified as the destination file to directly replace it. Note that the file "Factory_Default_Config.cfg" can be copied to the FTP/TFTP server, but cannot be used as the destination on the switch.

**Table 6: Flash/File Commands**

| Command | Function | Mode |
|---|---|---|
| boot system | Specifies the file or image used to start up the system | GC |
| copy | Copies a code image or a switch configuration to or from flash memory or an FTP/TFTP server | PE |
| delete | Deletes a file or code image | PE |
| dir | Displays a list of files in flash memory | PE |
| whichboot | Displays the files booted | PE |

**boot system** This command specifies the file or image used to start up the system.

### SYNTAX

**boot system** [*unit*:] {**boot-rom:** | **config:** | **opcode:**} *filename*

**boot-rom** - Boot ROM.

**config** - Configuration file.

**opcode** - Run-time operation code.

*filename* - Name of configuration file or code image.

### DEFAULT SETTING
None

### COMMAND MODE
Global Configuration

### COMMAND USAGE
■A colon (:) is required after the specified unit number and file type.

■If the file contains an error, it cannot be set as the default file.

### EXAMPLE

```
Console(config)#boot system config: startup
Console(config)#
```

### RELATED COMMANDS
dir (629)
whichboot (630)

**copy** This command moves (upload/download) a code image or configuration file between the switch's flash memory and an FTP/TFTP server. When you save the system code or configuration settings to a file on an FTP/TFTP server, that file can later be downloaded to the switch to restore system operation. The success of the file transfer depends on the accessibility of the FTP/TFTP server and the quality of the network connection.

### SYNTAX

**copy file** {**file** | **ftp** | **running-config** | **startup-config** | **tftp** | **unit**}
**copy running-config** {**file** | **ftp** | **startup-config** | **tftp**}
**copy startup-config** {**file** | **ftp** | **running-config** | **tftp**}
**copy tftp** {**file** | **https-certificate** | **public-key** | **running-config** | **startup-config**}
**copy unit file**

**file** - Keyword that allows you to copy to/from a file.

**ftp** - Keyword that allows you to copy to/from an FTP server.

**https-certificate** - Keyword that allows you to copy the HTTPS secure site certificate.

**public-key** - Keyword that allows you to copy a SSH key from a TFTP server. (See "Secure Shell" on page 716.)

**running-config** - Keyword that allows you to copy to/from the current running configuration.

**startup-config** - The configuration used for system initialization.

**tftp** - Keyword that allows you to copy to/from a TFTP server.

### DEFAULT SETTING
None

### COMMAND MODE
Privileged Exec

### COMMAND USAGE
- The system prompts for data required to complete the copy command.
- The destination file name should not contain slashes (\ or /), and the maximum length for file names is 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-")
- The switch supports only two operation code files, but the maximum number of user-defined configuration files is 16.
- You can use "Factory_Default_Config.cfg" as the source to copy from the factory default configuration file, but you cannot use it as the destination.
- To replace the startup configuration, you must use **startup-config** as the destination.
- The Boot ROM and Loader cannot be uploaded or downloaded from the FTP/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 266. For information on configuring the switch to use HTTPS for a secure connection, see the ip http secure-server command.
- When logging into an FTP server, the interface prompts for a user name and password configured on the remote server. Note that "anonymous" is set as the default user name.

### EXAMPLE
The following example shows how to download new firmware from a TFTP server:

```
Console#copy tftp file
TFTP server ip address: 10.1.0.19
Choose file type:
 1. config:  2. opcode: 2
Source file name: m360.bix
Destination file name: m360.bix
\Write to FLASH Programming.
-Write to FLASH finish.
```

```
Success.
Console#
```

The following example shows how to upload the configuration settings to a file on the TFTP server:

```
Console#copy file tftp
Choose file type:
 1. config:  2. opcode: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
TFTP completed.
Success.

Console#
```

The following example shows how to copy the running configuration to a startup file.

```
Console#copy running-config file
destination file name: startup
Write to FLASH Programming.
\Write to FLASH finish.
Success.

Console#
```

The following example shows how to download a configuration file:

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
Write to FLASH Programming.

\Write to FLASH finish.
Success.

Console#
```

This example shows how to copy a secure-site certificate from an TFTP server. It then reboots the switch to activate the certificate:

```
Console#copy tftp https-certificate
TFTP server ip address: 10.1.0.19
Source certificate file name: SS-certificate
Source private file name: SS-private
Private password: ********

Success.
Console#reload
System will be restarted, continue <y/n>? y
```

This example shows how to copy a public-key used by SSH from an TFTP server. Note that public key authentication via SSH is only supported for users configured locally on the switch.

```
Console#copy tftp public-key
TFTP server IP address: 192.168.1.19
Choose public key type:
 1. RSA:  2. DSA: <1-2>: 1
Source file name: steve.pub
Username: steve
TFTP Download
Success.
Write to FLASH Programming.
Success.

Console#
```

This example shows how to copy a file to an FTP server.

```
Console#copy ftp file
FTP server IP address: 169.254.1.11
User[anonymous]: admin
Password[]: *****
Choose file type:
 1. config:  2. opcode: 2
Source file name: BLANC.BIX
Destination file name: BLANC.BIX
Console#
```

## delete

This command deletes a file or image.

### SYNTAX

**delete** [*unit*:] *filename*

*filename* - Name of configuration file or code image.

### 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.

```
Console#delete test2.cfg
Console#
```

#### RELATED COMMANDS
dir (629)
delete public-key (721)

## dir
This command displays a list of files in flash memory.

#### SYNTAX
**dir** [*unit*:] {**boot-rom:** | **config:** | **opcode:**} [*filename*]}

**boot-rom** - Boot ROM (or diagnostic) image file.

**config** - Switch configuration file.

**opcode** - Run-time operation code image file.

*filename* - Name of configuration file or code image. If this file exists but contains errors, information on this file cannot be shown.

#### DEFAULT SETTING
None

#### COMMAND MODE
Privileged Exec

#### COMMAND USAGE
■If you enter the command **dir** without any parameters, the system displays all files.

■A colon (:) is required after the specified unit number and file type.

File information is shown below:

**Table 7: File Directory Information**

| Column Heading | Description |
|---|---|
| File Name | The name of the file. |
| Type | File types: Boot-Rom, Operation Code, and Config file. |
| Startup | Shows if this file is used when the system is started. |
| Modify Time | The date and time the file was last modified. |
| Size | The length of the file in bytes. |

#### EXAMPLE
The following example shows how to display all file information:

```
Console#dir
      File Name                    Type  Startup Modify Time        Size(bytes)
-------------------------- -------------- ------- ------------------- ----------
 Unit 1:
```

```
EL326_V1.2.1.0.BIX     OpCode    N    2010-03-12 07:15:13   15052008
EL326_V1.2.1.2.BIX     OpCode    Y    2010-04-23 11:50:11   15110656
Factory_Default_Config.cfg      Config    N    2009-10-12 12:02:08       455
startup1.cfg                    Config    Y    2010-06-22 02:48:51      4549
 ------------------------------------------------------------------------
                    Free space for compressed user config files:  10747904
Console#
```

## whichboot

This command displays which files were booted when the system powered up.

### SYNTAX

**whichboot**

### DEFAULT SETTING

None

### COMMAND MODE

Privileged Exec

### EXAMPLE

This example shows the information displayed by the **whichboot** command. See the table under the **dir** command for a description of the file information displayed by this command.

```
Console#whichboot
       File Name                Type  Startup Modify Time        Size(bytes)
-------------------------------- ------- ------- ------------------- -----------
 Unit 1:
EL326_V1.2.1.2.BIX     OpCode    Y    2010-04-23 11:50:11   15110656
startup1.cfg                    Config    Y    2009-12-09 08:43:18      3834
Console#
```

# LINE

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

**Table 8: Line Commands**

| Command | Function | Mode |
|---|---|---|
| line | Identifies a specific line for configuration and starts the line configuration mode | GC |
| accounting exec | Applies an accounting method to local console, Telnet or SSH connections | LC |
| authorization exec | Applies an authorization method to local console, Telnet or SSH connections | LC |
| databits* | Sets the number of data bits per character that are interpreted and generated by hardware | LC |

**Table 8: Line Commands (Continued)**

| Command | Function | Mode |
|---|---|---|
| exec-timeout | Sets the interval that the command interpreter waits until user input is detected | LC |
| login | Enables password checking at login | LC |
| parity* | Defines the generation of a parity bit | LC |
| password | Specifies a password on a line | LC |
| password-thresh | Sets the password intrusion threshold, which limits the number of failed logon attempts | LC |
| silent-time[1] | Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the password-thresh command | LC |
| speed* | Sets the terminal baud rate | LC |
| stopbits* | Sets the number of the stop bits transmitted per byte | LC |
| timeout login response | Sets the interval that the system waits for a login attempt | LC |
| disconnect | Terminates a line connection | PE |
| show line | Displays a terminal line's parameters | NE, PE |

1. These commands only apply to the serial port.

## line

This command identifies a specific line for configuration, and to process subsequent line configuration commands.

### SYNTAX

**line** {**console** | **vty**}

**console** - Console terminal line.

**vty** - Virtual terminal for remote console access (i.e., Telnet).

### DEFAULT SETTING

There is no default line.

### COMMAND MODE

Global Configuration

### COMMAND USAGE

Telnet is considered a virtual terminal connection and will be shown as “VTY” in screen displays such as show users. However, the serial communication parameters (e.g., databits) do not affect Telnet connections.

### EXAMPLE

To enter console line mode, enter the following command:

```
Console(config)#line console
Console(config-line)#
```

#### RELATED COMMANDS
show line (639)
show users (621)

## databits

This command sets the number of data bits per character that are interpreted and generated by the console port. Use the **no** form to restore the default value.

#### SYNTAX

**databits** {**7** | **8**}

**no databits**

7 - Seven data bits per character.

8 - Eight data bits per character.

#### DEFAULT SETTING
8 data bits per character

#### COMMAND MODE
Line Configuration

#### COMMAND USAGE
The **databits** command can be used to mask the high bit on input from devices that generate 7 data bits with parity. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character.

#### EXAMPLE
To specify 7 data bits, enter this command:

```
Console(config-line)#databits 7
Console(config-line)#
```

#### RELATED COMMANDS
parity (634)

## exec-timeout

This command sets the interval that the system waits until user input is detected. Use the **no** form to restore the default.

#### SYNTAX

**exec-timeout** [*seconds*]

**no exec-timeout**

*seconds* - Integer that specifies the timeout interval.
(Range: 0 - 65535 seconds; 0: no timeout)

#### DEFAULT SETTING

CLI: No timeout
Telnet: 10 minutes

#### COMMAND MODE

Line Configuration

#### COMMAND USAGE

- If user input is detected within the timeout interval, the session is kept open; otherwise the session is terminated.
- This command applies to both the local console and Telnet connections.
- The timeout for Telnet cannot be disabled.
- Using the command without specifying a timeout restores the default setting.

#### EXAMPLE

To set the timeout to two minutes, enter this command:

```
Console(config-line)#exec-timeout 120
Console(config-line)#
```

### login

This command enables password checking at login. Use the **no** form to disable password checking and allow connections without a password.

#### SYNTAX

**login** [**local**]

**no login**

**local** - Selects local password checking. Authentication is based on the user name specified with the username command.

#### DEFAULT SETTING

login local

#### COMMAND MODE

Line Configuration

#### COMMAND USAGE

- There are three authentication modes provided by the switch itself at login:
  - **login** selects authentication by a single global password as specified by the password line configuration command. When using this method, the management interface starts in Normal Exec (NE) mode.
  - **login local** selects authentication via the user name and password specified by the username command (i.e., default setting). When using this method, the

management interface starts in Normal Exec (NE) or Privileged Exec (PE) mode, depending on the user's privilege level (0 or 15 respectively).

- **no login** selects no authentication. When using this method, the management interface starts in Normal Exec (NE) mode.

- This command controls login authentication via the switch itself. To configure user names and passwords for remote authentication servers, you must use the RADIUS or TACACS software installed on those servers.

### EXAMPLE

```
Console(config-line)#login local
Console(config-line)#
```

### RELATED COMMANDS

username (692)
password (635)

## parity

This command defines the generation of a parity bit. Use the **no** form to restore the default setting.

### SYNTAX

**parity** {**none** | **even** | **odd**}

**no parity**

**none** - No parity

**even** - Even parity

**odd** - Odd parity

### DEFAULT SETTING

No parity

### COMMAND MODE

Line Configuration

### COMMAND USAGE

Communication protocols provided by devices such as terminals and modems often require a specific parity bit setting.

### EXAMPLE

To specify no parity, enter this command:

```
Console(config-line)#parity none
Console(config-line)#
```

## password

This command specifies the password for a line. Use the **no** form to remove the password.

### SYNTAX

**password** {**0** | **7**} *password*

**no password**

{**0** | **7**} - 0 means plain password, 7 means encrypted password

*password* - Character string that specifies the line password. (Maximum length: 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 an FTP/TFTP server. There is no need for you to manually configure encrypted passwords.

### EXAMPLE

```
Console(config-line)#password 0 secret
Console(config-line)#
```

### RELATED COMMANDS

login (633)
password-thresh (635)

## password-thresh

This command sets the password intrusion threshold which limits the number of failed logon attempts. Use the **no** form to remove the threshold value.

### SYNTAX

**password-thresh** [*threshold*]

**no password-thresh**

*threshold* - The number of allowed password attempts. (Range: 1-120; 0: no threshold)

#### DEFAULT SETTING

The default value is three attempts.

#### COMMAND MODE

Line Configuration

#### COMMAND USAGE

When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the silent-time command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface shuts down.

#### EXAMPLE

To set the password threshold to five attempts, enter this command:

```
Console(config-line)#password-thresh 5
Console(config-line)#
```

#### RELATED COMMANDS

silent-time (636)

## 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 (console only)

#### EXAMPLE

To set the silent time to 60 seconds, enter this command:

```
Console(config-line)#silent-time 60
Console(config-line)#
```

#### RELATED COMMANDS

password-thresh (635)

## 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

115200 bps

### COMMAND MODE

Line Configuration

### COMMAND USAGE

Set the speed to match the baud rate of the device connected to the serial port. Some baud rates available on devices connected to the port might not be supported. The system indicates if the speed you selected is not supported.

### EXAMPLE

To specify 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**}

**no stopbits**

1 - One stop bit

2 - Two stop bits

### DEFAULT SETTING

1 stop bit

### COMMAND MODE

Line Configuration

### EXAMPLE

To specify 2 stop bits, enter this command:

```
Console(config-line)#stopbits 2
Console(config-line)#
```

## timeout login response

This command sets the interval that the system waits for a user to log into the CLI. Use the **no** form to restore the default setting.

### SYNTAX

**timeout login response** [*seconds*]

**no timeout login response**

*seconds* - Integer that specifies the timeout interval. (Range: 0 - 300 seconds; 0: disabled)

### DEFAULT SETTING

CLI: Disabled (0 seconds)
Telnet: 300 seconds

### COMMAND MODE

Line Configuration

### COMMAND USAGE

- If a login attempt is not detected within the timeout interval, the connection is terminated for the session.
- This command applies to both the local console and Telnet connections.
- The timeout for Telnet cannot be disabled.
- Using the command without specifying a timeout restores the default setting.

### EXAMPLE

To set the timeout to two minutes, enter this command:

```
Console(config-line)#timeout login response 120
Console(config-line)#
```

## disconnect

This command terminates an SSH, Telnet, or console connection.

### SYNTAX

**disconnect** *session-id*

*session-id* – The session identifier for an SSH, Telnet or console connection. (Range: 0-4)

### COMMAND MODE

Privileged Exec

### COMMAND USAGE

Specifying session identifier “0” will disconnect the console connection. Specifying any other identifiers for an active session will disconnect an SSH or Telnet connection.

### EXAMPLE

```
Console#disconnect 1
Console#
```

### RELATED COMMANDS

show ssh (725)
show users (621)

## show line

This command displays the terminal line’s parameters.

### SYNTAX

**show line** [**console** | **vty**]

**console** - Console terminal line.

**vty** - Virtual terminal for remote console access (i.e., Telnet).

### DEFAULT SETTING

Shows all lines

### COMMAND MODE

Normal Exec, Privileged Exec

### EXAMPLE

To show all lines, enter this command:

```
Console#show line
 Console Configuration:
  Password Threshold : 3 times
  Inactive Timeout   : Disabled
  Login Timeout      : Disabled
  Silent Time        : Disabled
  Baud Rate          : 115200
  Data Bits          : 8
  Parity             : None
  Stop Bits          : 1

 VTY Configuration:
  Password Threshold : 3 times
  Inactive Timeout   : 600 sec.
  Login Timeout      : 300 sec.
  Silent Time        : Disabled
Console#
```

# EVENT LOGGING

This section describes commands used to configure event logging on the switch.

**Table 9: Event Logging Commands**

| Command | Function | Mode |
|---|---|---|
| logging facility | Sets the facility type for remote logging of syslog messages | GC |
| logging history | Limits syslog messages saved to switch memory based on severity | GC |
| logging host | Adds a syslog server host IP address that will receive logging messages | GC |
| logging on | Controls logging of error messages | GC |
| logging trap | Limits syslog messages saved to a remote server based on severity | GC |
| clear log | Clears messages from the logging buffer | PE |
| show log | Displays log messages | PE |
| show logging | Displays the state of logging | PE |

## logging facility

This command sets the facility type for remote logging of syslog messages. Use the **no** form to return the type to the default.

### SYNTAX

**logging facility** *type*

**no logging facility**

*type* - A number that indicates the facility used by the syslog server to dispatch log messages to an appropriate service. (Range: 16-23)

### DEFAULT SETTING

23

### COMMAND MODE

Global Configuration

### COMMAND USAGE

The command specifies the facility type tag sent in syslog messages. (See RFC 3164.) This type has no effect on the kind of messages reported by the switch. However, it may be used by the syslog server to sort messages or to store messages in the corresponding database.

### EXAMPLE

```
Console(config)#logging facility 19
Console(config)#
```

## logging history

This command limits syslog messages saved to switch memory based on severity. The **no** form returns the logging of syslog messages to the default level.

### SYNTAX

**logging history** {**flash** | **ram**} *level*

**no logging history** {**flash** | **ram**}

**flash** - Event history stored in flash memory (i.e., permanent memory).

**ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).

*level* - One of the levels listed below. Messages sent include the selected level down to level 0. (Range: 0-7)

**Table 10: Logging Levels**

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

### DEFAULT SETTING

Flash: errors (level 3 - 0)
RAM: debugging (level 7 - 0)

### COMMAND MODE

Global Configuration

### COMMAND USAGE

The message level specified for flash memory must be a higher priority (i.e., numerically lower) than that specified for RAM.

### EXAMPLE

```
Console(config)#logging history ram 0
Console(config)#
```

## logging host

This command adds a syslog server host IP address that will receive logging messages. Use the **no** form to remove a syslog server host.

#### SYNTAX

[**no**] **logging host** *host-ip-address*

*host-ip-address* - The IPv4 or IPv6 address of a syslog server.

#### DEFAULT SETTING

None

#### COMMAND MODE

Global Configuration

#### COMMAND USAGE

■Use this command more than once to build up a list of host IP addresses.

■The maximum number of host IP addresses allowed is five.

#### EXAMPLE

```
Console(config)#logging host 10.1.0.3
Console(config)#
```

## logging on

This command controls logging of error messages, sending debug or error messages to a logging process. The **no** form disables the logging process.

#### SYNTAX

[**no**] **logging on**

#### DEFAULT SETTING

None

#### COMMAND MODE

Global Configuration

#### COMMAND USAGE

The logging process controls error messages saved to switch memory or sent to remote syslog servers. You can use the logging history command to control the type of error messages that are stored in memory. You can use the logging trap command to control the type of error messages that are sent to specified syslog servers.

#### EXAMPLE

```
Console(config)#logging on
Console(config)#
```

### RELATED COMMANDS

logging history (641)
logging trap (643)
clear log (643)

## logging trap

This command enables the logging of system messages to a remote server, or limits the syslog messages saved to a remote server based on severity. Use this command without a specified level to enable remote logging. Use the **no** form to disable remote logging.

### SYNTAX

**logging trap** [**level** *level*]

**no logging trap** [**level**]

*level* - One of the syslog severity levels listed in the table on page 641. Messages sent include the selected level through level 0.

### DEFAULT SETTING

Disabled
Level 7

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- Using this command with a specified level enables remote logging and sets the minimum severity level to be saved.
- Using this command without a specified level also enables remote logging, but restores the minimum severity level to the default.

### EXAMPLE

```
Console(config)#logging trap 4
Console(config)#
```

## clear log

This command clears messages from the log buffer.

### SYNTAX

**clear log** [**flash** | **ram**]

**flash** - Event history stored in flash memory (i.e., permanent memory).

**ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).

### DEFAULT SETTING

Flash and RAM

### COMMAND MODE
Privileged Exec

### EXAMPLE

```
Console#clear log
Console#
```

### RELATED COMMANDS
show log (644)

## show log

This command displays the log messages stored in local memory.

### SYNTAX

**show log** {**flash** | **ram**}

**flash** - Event history stored in flash memory (i.e., permanent memory).

**ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).

### DEFAULT SETTING
None

### COMMAND MODE
Privileged Exec

### EXAMPLE
The following example shows the event message stored in RAM.

```
Console#show log ram
[1] 00:01:30 2001-01-01
  "VLAN 1 link-up notification."
  level: 6, module: 5, function: 1, and event no.: 1
[0] 00:01:30 2001-01-01
  "Unit 1, Port  1 link-up notification."
  level: 6, module: 5, function: 1, and event no.: 1
Console#
```

## show logging

This command displays the configuration settings for logging messages to local switch memory, to an SMTP event handler, or to a remote syslog server.

### SYNTAX

**show logging** {**flash** | **ram** | **sendmail** | **trap**}

**flash** - Displays settings for storing event messages in flash memory (i.e., permanent memory).

**ram** - Displays settings for storing event messages in temporary RAM (i.e., memory flushed on power reset).

**sendmail** - Displays settings for the SMTP event handler (page 649).

**trap** - Displays settings for the trap function.

### DEFAULT SETTING
None

### COMMAND MODE
Privileged Exec

### EXAMPLE
The following example shows that system logging is enabled, the message level for flash memory is “errors” (i.e., default level 3 - 0), and the message level for RAM is “debugging” (i.e., default level 7 - 0).

```
Console#show logging flash
Syslog logging:          Enabled
History logging in FLASH: level errors
Console#show logging ram
Syslog logging:          Enabled
History logging in RAM: level debugging
Console#
```

**Table 11: 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
Remote Log Status          : Disabled
Remote Log Facility Type    : Local use 7
Remote Log Level Type       : Debugging messages
Remote Log Server IP Address : 0.0.0.0
Remote Log Server IP Address : 0.0.0.0
Remote Log Server IP Address : 0.0.0.0
Remote Log Server IP Address : 0.0.0.0
Remote Log Server IP Address : 0.0.0.0
Console#
```

**Table 12: 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. |

**Table 12: show logging trap** - display description

| Field | Description |
|---|---|
| REMOTELOG level type | The severity threshold for syslog messages sent to a remote server as specified in the logging trap command. |
| REMOTELOG server IP address | The address of syslog servers as specified in the logging host command. |

### RELATED COMMANDS

show logging sendmail (649)

## SMTP ALERTS

These commands configure SMTP event handling, and forwarding of alert messages to the specified SMTP servers and email recipients.

**Table 13: Event Logging Commands**

| Command | Function | Mode |
|---|---|---|
| logging sendmail | Enables SMTP event handling | GC |
| logging sendmail host | SMTP servers to receive alert messages | GC |
| logging sendmail level | Severity threshold used to trigger alert messages | GC |
| logging sendmail destination-email | Email recipients of alert messages | GC |
| logging sendmail source-email | Email address used for “From” field of alert messages | GC |
| show logging sendmail | Displays SMTP event handler settings | NE, PE |

### logging sendmail

This command enables SMTP event handling. Use the **no** form to disable this function.

### SYNTAX

[**no**] **logging sendmail**

### DEFAULT SETTING

Enabled

### COMMAND MODE

Global Configuration

### EXAMPLE

```
Console(config)#logging sendmail
Console(config)#
```

## logging sendmail host

This command specifies SMTP servers that will be sent alert messages. Use the **no** form to remove an SMTP server.

### SYNTAX

[**no**] **logging sendmail host** *ip-address*

*ip-address* - IP address of an SMTP server that will be sent alert messages for event handling.

### DEFAULT SETTING

None

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- You can specify up to three SMTP servers for event handing. However, you must enter a separate command to specify each server.
- To send email alerts, the switch first opens a connection, sends all the email alerts waiting in the queue one by one, and finally closes the connection.
- To open a connection, the switch first selects the server that successfully sent mail during the last connection, or the first server configured by this command. If it fails to send mail, the switch selects the next server in the list and tries to send mail again. If it still fails, the system will repeat the process at a periodic interval. (A trap will be triggered if the switch cannot successfully open a connection.)

### EXAMPLE

```
Console(config)#logging sendmail host 192.168.1.19
Console(config)#
```

## logging sendmail level

This command sets the severity threshold used to trigger alert messages. Use the **no** form to restore the default setting.

### SYNTAX

**logging sendmail level** *level*

**no logging sendmail level**

*level* - One of the system message levels (page 641). Messages sent include the selected level down to level 0. (Range: 0-7; Default: 7)

### DEFAULT SETTING

Level 7

### COMMAND MODE

Global Configuration

#### Command Usage

The specified level indicates an event threshold. All events at this level or higher will be sent to the configured email recipients. (For example, using Level 7 will report all events from level 7 to level 0.)

#### Example

This example will send email alerts for system errors from level 3 through 0.

```
Console(config)#logging sendmail level 3
Console(config)#
```

### logging sendmail 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 source-email

This command sets the email address used for the “From” field in alert messages. Use the **no** form to restore the default value.

#### Syntax

**logging sendmail source-email** email-address

**no logging sendmail source-email**

*email-address* - The source email address used in alert messages. (Range: 1-41 characters)

#### Default Setting

None

### COMMAND MODE
Global Configuration

### COMMAND USAGE
You may use an symbolic email address that identifies the switch, or the address of an administrator responsible for the switch.

### EXAMPLE

```
Console(config)#logging sendmail source-email bill@this-company.com
Console(config)#
```

## show logging sendmail

This command displays the settings for the SMTP event handler.

### COMMAND MODE
Normal Exec, Privileged Exec

### EXAMPLE

```
Console#show logging sendmail
SMTP servers
-----------------------------------------------
  1. 192.168.1.19

SMTP Minimum Severity Level: 7

SMTP destination email addresses
-----------------------------------------------
   1. ted@this-company.com

SMTP Source E-mail Address: bill@this-company.com

SMTP Status: Enabled
Console#
```

# TIME

The system clock can be dynamically set by polling a set of specified time servers (NTP or SNTP). Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. If the clock is not set, the switch will only record the time from the factory default set at the last bootup.

**Table 14: Time Commands**

| Command | Function | Mode |
|---|---|---|
| *SNTP Commands* | | |
| sntp client | Accepts time from specified time servers | GC |
| sntp poll | Sets the interval at which the client polls for time | GC |
| sntp server | Specifies one or more time servers | GC |
| show sntp | Shows current SNTP configuration settings | NE, PE |

**Table 14: Time Commands (Continued)**

| Command | Function | Mode |
|---|---|---|
| *Manual Configuration Commands* | | |
| clock timezone | Sets the time zone for the switch's internal clock | GC |
| calendar set | Sets the system date and time | PE |
| show calendar | Displays the current date and time setting | NE, PE |

## sntp client

This command enables SNTP client requests for time synchronization from NTP or SNTP time servers specified with the sntp server command. Use the **no** form to disable SNTP client requests.

### SYNTAX

[**no**] **sntp client**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- The time acquired from time servers is used to record accurate dates and times for log events. Without SNTP, the switch only records the time starting from the factory default set at the last bootup (i.e., 00:00:00, Jan. 1, 2001).
- This command enables client time requests to time servers specified via the sntp server command. It issues time synchronization requests based on the interval set via the sntp poll command.

### EXAMPLE

```
Console(config)#sntp server 10.1.0.19
Console(config)#sntp poll 60
Console(config)#sntp client
Console(config)#end
Console#show sntp
Current Time:  Dec 23 02:52:44 2002
Poll Interval: 60
Current Mode: unicast
SNTP Status : Enabled
SNTP Server 137.92.140.80 0.0.0.0 0.0.0.0
Current Server: 137.92.140.80
Console#
```

### RELATED COMMANDS

sntp server (651)
sntp poll (651)
show sntp (652)

## sntp poll

This command sets the interval between sending time requests when the switch is set to SNTP client mode. Use the **no** form to restore to the default.

### SYNTAX

**sntp poll** *seconds*

**no sntp poll**

*seconds* - Interval between time requests. (Range: 16-16384 seconds)

### DEFAULT SETTING

16 seconds

### COMMAND MODE

Global Configuration

### EXAMPLE

```
Console(config)#sntp poll 60
Console#
```

### RELATED COMMANDS

sntp client (650)

## sntp server

This command sets the IP address of the servers to which SNTP time requests are issued. Use the this command with no arguments to clear all time servers from the current list. Use the **no** form to clear all time servers from the current list, or to clear a specific server.

### SYNTAX

**sntp server** [*ip1* [*ip2* [*ip3*]]]

**no sntp server** [*ip1* [*ip2* [*ip3*]]]

*ip* - IPv4 or IPv6 address of an time server (NTP or SNTP).
(Range: 1 - 3 addresses)

### DEFAULT SETTING

None

### COMMAND MODE

Global Configuration

### COMMAND USAGE

This command specifies time servers from which the switch will poll for time updates when set to SNTP client mode. The client will poll the time servers in the order specified until a response is received. It issues time synchronization requests based on the interval set via the sntp poll command.

### EXAMPLE

```
Console(config)#sntp server 10.1.0.19
Console#
```

### RELATED COMMANDS

sntp client (650)
sntp poll (651)
show sntp (652)

## show sntp

This command displays the current time and configuration settings for the SNTP client, and indicates whether or not the local time has been properly updated.

### COMMAND MODE

Normal Exec, Privileged Exec

### COMMAND USAGE

This command displays the current time, the poll interval used for sending time synchronization requests, and the current SNTP mode (i.e., unicast).

### EXAMPLE

```
Console#show sntp
Current Time   : Nov  5 18:51:22 2006
Poll Interval  : 16 seconds
Current Mode   : Unicast
SNTP Status    : Enabled
SNTP Server    : 137.92.140.80
                 137.92.140.81
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: 1-30 characters)

*hours* - Number of hours before/after UTC. (Range: 0-12 hours before UTC, 0-13 hours after UTC)

*minutes* - Number of minutes before/after UTC. (Range: 0-59 minutes)

**before-utc** - Sets the local time zone before (east) of UTC.

**after-utc** - Sets the local time zone after (west) of UTC.

### DEFAULT SETTING

None

#### COMMAND MODE
Global Configuration

#### COMMAND USAGE
This command sets the local time zone relative to the Coordinated Universal Time (UTC, formerly Greenwich Mean Time or GMT), based on the earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

#### EXAMPLE

```
Console(config)#clock timezone Japan hours 8 minute 0 after-UTC
Console(config)#
```

#### RELATED COMMANDS
show sntp (652)

### calendar set

This command sets the system clock. It may be used if there is no time server on your network, or if you have not configured the switch to receive signals from a time server.

#### SYNTAX

**calendar set** *hour min sec* {*day month year* | *month day year*}

*hour* - Hour in 24-hour format. (Range: 0 - 23)

*min* - Minute. (Range: 0 - 59)

*sec* - Second. (Range: 0 - 59)

*day* - Day of month. (Range: 1 - 31)

*month* - **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**

*year* - Year (4-digit). (Range: 2001 - 2100)

#### DEFAULT SETTING
None

#### COMMAND MODE
Privileged Exec

#### COMMAND USAGE
Note that when SNTP is enabled, the system clock cannot be manually configured.

#### EXAMPLE
This example shows how to set the system clock to 15:12:34, February 1st, 2002.

```
Console#calendar set 15:12:34 1 February 2002
Console#
```

**show calendar** This command displays the system clock.

#### DEFAULT SETTING
None

#### COMMAND MODE
Normal Exec, Privileged Exec

#### EXAMPLE

```
Console#show calendar
 15:12:34 February 1 2002
Console#
```

## TIME RANGE

This section describes the commands used to sets a time range for use by other functions, such as Access Control Lists.

**Table 15: Time Range Commands**

| Command | Function | Mode |
|---|---|---|
| time-range | Specifies the name of a time range, and enters time range configuration mode | GC |
| absolute | Sets the time range for the execution of a command | TR |
| periodic | Sets the time range for the periodic execution of a command | TR |
| show time-range | Shows configured time ranges. | PE |

**time-range** This command specifies the name of a time range, and enters time range configuration mode. Use the **no** form to remove a previously specified time range.

#### SYNTAX

[**no**] **time-range** *name*

*name* - Name of the time range. (Range: 1-30 characters)

#### DEFAULT SETTING
None

#### COMMAND MODE
Global Configuration

#### COMMAND USAGE
This command sets a time range for use by other functions, such as Access Control Lists.

### EXAMPLE

```
Console(config)#time-range r&d
Console(config-time-range)#
```

### RELATED COMMANDS

Access Control Lists (783)

## absolute

This command sets the time range for the execution of a command. Use the **no** form to remove a previously specified time.

### SYNTAX

**absolute start** *hour minute day month year*
[**end** *hour minutes day month year*]

**absolute end** *hour minutes day month year*

**no absolute**

*hour* - Hour in 24-hour format. (Range: 0-23)

*minute* - Minute. (Range: 0-59)

*day* - Day of month. (Range: 1-31)

*month* - **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**

*year* - Year (4-digit). (Range: 2009-2109)

### DEFAULT SETTING

None

### COMMAND MODE

Time Range Configuration

### COMMAND USAGE

If a time range is already configured, you must use the **no** form of this command to remove the current entry prior to configuring a new time range.

### EXAMPLE

This example configures the time for the single occurrance of an event.

```
Console(config)#time-range r&d
Console(config-time-range)#absolute start 1 1 1 april 2009 end 2 1 1 april 2009
Console(config-time-range)#
```

## periodic

This command sets the time range for the periodic execution of a command. Use the **no** form to remove a previously specified time range.

#### SYNTAX

[**no**] **periodic** {**daily** | **friday** | **monday** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday** | **weekdays** | **weekend**} *hour minute* to {**daily** | **friday** | **monday** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday** | **weekdays** | **weekend** | *hour minute*}

**daily** - Daily

**friday** - Friday

**monday** - Monday

**saturday** - Saturday

**sunday** - Sunday

**thursday** - Thursday

**tuesday** - Tuesday

**wednesday** - Wednesday

**weekdays** - Weekdays

**weekend** - Weekends

*hour* - Hour in 24-hour format. (Range: 0-23)

*minute* - Minute. (Range: 0-59)

#### DEFAULT SETTING
None

#### COMMAND MODE
Time Range Configuration

#### EXAMPLE
This example configures a time range for the periodic occurrance of an event.

```
Console(config)#time-range sales
Console(config-time-range)#periodic daily 1 1 to 2 1
Console(config-time-range)#
```

## show time-range

This command shows configured time ranges.

#### SYNTAX

**show time-range** [*name*]

*name* - Name of the time range. (Range: 1-30 characters)

#### DEFAULT SETTING
None

#### COMMAND MODE
Privileged Exec

### EXAMPLE

```
Console#show time-range r&d
 Time-range r&d:
   absolute start 01:01 01 April 2009
   periodic    Daily 01:01 to    Daily 02:01
   periodic    Daily 02:01 to    Daily 03:01

Console#
```

# 26 SNMP COMMANDS

Controls access to this switch from management stations using the Simple Network Management Protocol (SNMP), as well as the error types sent to trap managers.

SNMP Version 3 also provides security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree. To use SNMPv3, first set an SNMP engine ID (or accept the default), specify read and write access views for the MIB tree, configure SNMP user groups with the required security model (i.e., SNMP v1, v2c or v3) and security level (i.e., authentication and privacy), and then assign SNMP users to these groups, along with their specific authentication and privacy passwords.

**Table 1: SNMP Commands**

| Command | Function | Mode |
|---|---|---|
| *General SNMP Commands* | | |
| snmp-server | Enables the SNMP agent | GC |
| snmp-server community | Sets up the community access string to permit access to SNMP commands | GC |
| snmp-server contact | Sets the system contact string | GC |
| snmp-server location | Sets the system location string | GC |
| show snmp | Displays the status of SNMP communications | NE, PE |
| *SNMP Target Host Commands* | | |
| snmp-server enable traps | Enables the device to send SNMP traps (i.e., SNMP notifications) | GC |
| snmp-server host | Specifies the recipient of an SNMP notification operation | GC |
| *SNMPv3 Engine Commands* | | |
| snmp-server engine-id | Sets the SNMP engine ID | GC |
| snmp-server group | Adds an SNMP group, mapping users to views | GC |
| snmp-server user | Adds a user to an SNMP group | GC |
| snmp-server view | Adds an SNMP view | GC |
| show snmp engine-id | Shows the SNMP engine ID | PE |
| show snmp group | Shows the SNMP groups | PE |
| show snmp user | Shows the SNMP users | PE |
| show snmp view | Shows the SNMP views | PE |
| *Notification Log Commands* | | |
| nlm | Enables the specified notification log | GC |
| snmp-server notify-filter | Creates a notification log and specifies the target host | GC |
| show nlm oper-status | Shows operation status of configured notification logs | PE |

**Table 1: SNMP Commands (Continued)**

| Command | Function | Mode |
|---|---|---|
| show snmp notify-filter | Displays the configured notification logs | PE |
| *ATC Trap Commands* | | |
| snmp-server enable port-traps atc broadcast-alarm-clear | Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered | IC (Port) |
| snmp-server enable port-traps atc broadcast-alarm-fire | Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control | IC (Port) |
| snmp-server enable port-traps atc broadcast-control-apply | Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control and the apply timer expires | IC (Port) |
| snmp-server enable port-traps atc broadcast-control-release | Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires | IC (Port) |
| snmp-server enable port-traps atc multicast-alarm-clear | Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered | IC (Port) |
| snmp-server enable port-traps atc multicast-alarm-fire | Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control | IC (Port) |
| snmp-server enable port-traps atc multicast-control-apply | Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control and the apply timer expires | IC (Port) |
| snmp-server enable port-traps atc multicast-control-release | Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires | IC (Port) |

## snmp-server

This command enables the SNMPv3 engine and services for all management clients (i.e., versions 1, 2c, 3). Use the **no** form to disable the server.

### SYNTAX

[**no**] **snmp-server**

### DEFAULT SETTING

Enabled

### COMMAND MODE

Global Configuration

### EXAMPLE

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

## snmp-server community

This command defines community access strings used to authorize management access by clients using SNMP v1 or v2c. Use the **no** form to remove the specified community string.

### SYNTAX

**snmp-server community** *string* [**ro** | **rw**]

**no snmp-server community** *string*

*string* - Community string that acts like a password and permits access to the SNMP protocol. (Maximum length: 32 characters, case sensitive; Maximum number of strings: 5)

**ro** - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.

**rw** - Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

### DEFAULT SETTING

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

### COMMAND MODE

Global Configuration

### EXAMPLE

```
Console(config)#snmp-server community alpha rw
Console(config)#
```

## snmp-server contact

This command sets the system contact string. Use the **no** form to remove the system contact information.

### SYNTAX

**snmp-server contact** *string*

no snmp-server contact

*string* - String that describes the system contact information. (Maximum length: 255 characters)

### DEFAULT SETTING

None

### COMMAND MODE

Global Configuration

### EXAMPLE

```
Console(config)#snmp-server contact Paul
Console(config)#
```

### RELATED COMMANDS

snmp-server location (662)

## snmp-server location

This command sets the system location string. Use the **no** form to remove the location string.

### SYNTAX

**snmp-server location** *text*

**no snmp-server location**

*text* - String that describes the system location. (Maximum length: 255 characters)

### DEFAULT SETTING

None

### COMMAND MODE

Global Configuration

### EXAMPLE

```
Console(config)#snmp-server location WC-19
Console(config)#
```

### RELATED COMMANDS

snmp-server contact (661)

## show snmp

This command can be used to check the status of SNMP communications.

### DEFAULT SETTING

None

### COMMAND MODE

Normal Exec, Privileged Exec

### COMMAND USAGE

This command provides information on the community access strings, counter information for SNMP input and output protocol data units, and whether or not SNMP logging has been enabled with the **snmp-server enable traps** command.

### EXAMPLE

```
Console#show snmp

SNMP Agent : Enabled

SNMP Traps :
 Authentication : Enabled
 Link-up-down   : Enabled
```

```
SNMP Communities :
   1. public, and the access level is read-only
   2. private, and the access level is read/write

0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
0 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs

SNMP Logging: Disabled
Console#
```

## snmp-server enable traps

This command enables this device to send Simple Network Management Protocol traps or informs (i.e., SNMP notifications). Use the **no** form to disable SNMP notifications.

### SYNTAX

[**no**] **snmp-server enable traps** [**authentication** | **link-up-down**]

**authentication** - Keyword to issue authentication failure notifications.

**link-up-down** - Keyword to issue link-up or link-down notifications.

### 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.
- The authentication, link-up, and link-down traps are legacy notifications, and therefore when used for SNMP Version 3 hosts, they must be enabled in

conjunction with the corresponding entries in the Notify View assigned by the snmp-server group command.

#### EXAMPLE

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

#### RELATED COMMANDS

snmp-server host (664)

### snmp-server host

This command specifies the recipient of a Simple Network Management Protocol notification operation. Use the **no** form to remove the specified host.

#### SYNTAX

**snmp-server host** *host-addr* [**inform** [**retry** *retries* | **timeout** *seconds*]]
*community-string*
[**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} [**udp-port** *port*]}

**no snmp-server host** *host-addr*

*host-addr* - Internet address of the host (the targeted recipient). (Maximum host addresses: 5 trap destination IP address entries)

**inform** - Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)

*retries* - The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)

*seconds* - The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)

*community-string* - Password-like community string sent with the notification operation to SNMP V1 and V2c hosts. Although you can set this string using the **snmp-server host** command by itself, we recommend defining it with the snmp-server community command prior to using the **snmp-server host** command. (Maximum length: 32 characters)

**version** - Specifies whether to send notifications as SNMP Version 1, 2c or 3 traps. (Range: 1, 2c, 3; Default: 1)

**auth** | **noauth** | **priv** - This group uses SNMPv3 with authentication, no authentication, or with authentication and privacy. See "Simple Network Management Protocol" on page 343 for further information about these authentication and encryption options.

*port* - Host UDP port to use. (Range: 1-65535; Default: 162)

#### DEFAULT SETTING

Host Address: None
Notification Type: Traps
SNMP Version: 1
UDP Port: 162

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the switch to send SNMP notifications, you must enter at least one **snmp-server host** command. In order to enable multiple hosts, you must issue a separate **snmp-server host** command for each host.
- The **snmp-server host** command is used in conjunction with the snmp-server enable traps command. Use the snmp-server enable traps command to enable the sending of traps or informs and to specify which SNMP notifications are sent globally. For a host to receive notifications, at least one snmp-server enable traps command and the **snmp-server host** command for that host must be enabled.
- Some notification types cannot be controlled with the snmp-server enable traps command. For example, some notification types are always enabled.
- Notifications are issued by the switch as trap messages by default. The recipient of a trap message does not send a response to the switch. Traps are therefore not as reliable as inform messages, which include a request for acknowledgement of receipt. Informs can be used to ensure that critical information is received by the host. However, note that informs consume more system resources because they must be kept in memory until a response is received. Informs also add to network traffic. You should consider these effects when deciding whether to issue notifications as traps or informs.

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

  1. Enable the SNMP agent (page 660).
  2. Create a view with the required notification messages (page 669).
  3. Create a group that includes the required notify view (page 667).
  4. Allow the switch to send SNMP traps; i.e., notifications (page 663).
  5. Specify the target host that will receive inform messages with the **snmp-server host** command as described in this section.

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

  1. Enable the SNMP agent (page 660).
  2. Create a local SNMPv3 user to use in the message exchange process (page 668).
  3. Create a view with the required notification messages (page 669).
  4. Create a group that includes the required notify view (page 667).
  5. Allow the switch to send SNMP traps; i.e., notifications (page 663).
  6. Specify the target host that will receive inform messages with the **snmp-server host** command as described in this section.

- The switch can send SNMP Version 1, 2c or 3 notifications to a host IP address, depending on the SNMP version that the management station supports. If the **snmp-server host** command does not specify the SNMP version, the default is to send SNMP version 1 notifications.
- If you specify an SNMP Version 3 host, then the community string is interpreted as an SNMP user name. The user name must first be defined with the snmp-server user command. Otherwise, an SNMPv3 group will be automatically created by the **snmp-server host** command using the name of the specified community string, and default settings for the read, write, and notify view.

### EXAMPLE

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#
```

### RELATED COMMANDS

snmp-server enable traps (663)

## snmp-server engine-id

This command configures an identification string for the SNMPv3 engine. Use the **no** form to restore the default.

### SYNTAX

**snmp-server engine-id** {**local** | **remote** {*ip-address*}} *engineid-string*

**no snmp-server engine-id** {**local** | **remote** {*ip-address*}}

**local** - Specifies the SNMP engine on this switch.

**remote** - Specifies an SNMP engine on a remote device.

*ip-address* - The Internet address of the remote device.

*engineid-string* - String identifying the engine ID. (Range: 1-26 hexadecimal characters)

### DEFAULT SETTING

A unique engine ID is automatically generated by the switch based on its MAC address.

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- An SNMP engine is an independent SNMP agent that resides either on this switch or on a remote device. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.
- A remote engine ID is required when using SNMPv3 informs. (See the snmp-server host command.) The remote engine ID is used to compute the security digest for authentication and encryption of packets passed between the switch and a user on the remote host. SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it.
- Trailing zeroes need not be entered to uniquely specify a engine ID. In other words, the value "0123456789" is equivalent to "0123456789" followed by 16 zeroes for a local engine ID.
- A local engine ID is automatically generated that is unique to the switch. This is referred to as the default engine ID. If the local engine ID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users (page 668).

### EXAMPLE

```
Console(config)#snmp-server engine-id local 1234567890
Console(config)#snmp-server engineID remote 9876543210 192.168.1.19
Console(config)#
```

### RELATED COMMANDS

snmp-server host (664)

## snmp-server group

This command adds an SNMP group, mapping SNMP users to SNMP views. Use the **no** form to remove an SNMP group.

### SYNTAX

**snmp-server group** *groupname*
{**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}}
[**read** *readview*] [**write** *writeview*] [**notify** *notifyview*]

**no snmp-server group** *groupname*

*groupname* - Name of an SNMP group. (Range: 1-32 characters)

**v1** | **v2c** | **v3** - Use SNMP version 1, 2c or 3.

**auth** | **noauth** | **priv** - This group uses SNMPv3 with authentication, no authentication, or with authentication and privacy. See "Simple Network Management Protocol" on page 343 for further information about these authentication and encryption options.

*readview* - Defines the view for read access. (1-32 characters)

*writeview* - Defines the view for write access. (1-32 characters)

*notifyview* - Defines the view for notifications. (1-32 characters)

### DEFAULT SETTING

Default groups: public[1] (read only), private[2] (read/write)
*readview* - Every object belonging to the Internet OID space (1).
writeview - Nothing is defined.
*notifyview* - Nothing is defined.

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- A group sets the access policy for the assigned users.
- When authentication is selected, the MD5 or SHA algorithm is used as specified in the snmp-server user command.
- When privacy is selected, the DES 56-bit algorithm is used for data encryption.
- For additional information on the notification messages supported by this switch, see Table 7, "Supported Notification Messages," on page 352. Also, note that the authentication, link-up and link-down messages are legacy traps and must therefore be enabled in conjunction with the snmp-server enable traps command.

1. No view is defined.
2. Maps to the defaultview.

### EXAMPLE

```
Console(config)#snmp-server group r&d v3 auth write daily
Console(config)#
```

## snmp-server user

This command adds a user to an SNMP group, restricting the user to a specific SNMP Read, Write, or Notify View. Use the **no** form to remove a user from an SNMP group.

### SYNTAX

**snmp-server user** *username groupname* [**remote** *ip-address*] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password* [**priv des56** *priv-password*]]

**no snmp-server user** *username* {**v1** | **v2c** | **v3** | **remote**}

*username* - Name of user connecting to the SNMP agent. (Range: 1-32 characters)

groupname - Name of an SNMP group to which the user is assigned. (Range: 1-32 characters)

**remote** - Specifies an SNMP engine on a remote device.

*ip-address* - The Internet address of the remote device.

**v1** | **v2c** | **v3** - Use SNMP version 1, 2c or 3.

**encrypted** - Accepts the password as encrypted input.

**auth** - Uses SNMPv3 with authentication.

**md5** | **sha** - Uses MD5 or SHA authentication.

*auth-password* - Authentication password. Enter as plain text if the **encrypted** option is not used. Otherwise, enter an encrypted password. (A minimum of eight characters is required.)

**priv des56** - Uses SNMPv3 with privacy with DES56 encryption.

*priv-password* - Privacy password. Enter as plain text if the **encrypted** option is not used. Otherwise, enter an encrypted password.

### DEFAULT SETTING

None

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- Local users (i.e., the command does not specify a remote engine identifier) must be configured to authorize management access for SNMPv3 clients, or to identify the source of SNMPv3 trap messages sent from the local switch.
- Remote users (i.e., the command specifies a remote engine identifier) must be configured to identify the source of SNMPv3 inform messages sent from the local switch.

- The SNMP engine ID is used to compute the authentication/privacy digests from the password. You should therefore configure the engine ID with the snmp-server engine-id command before using this configuration command.
- Before you configure a remote user, use the snmp-server engine-id command to specify the engine ID for the remote device where the user resides. Then use the **snmp-server user** command to specify the user and the IP address for the remote device where the user resides. The remote agent's SNMP engine ID is used to compute authentication/privacy digests from the user's password. If the remote engine ID is not first configured, the **snmp-server user** command specifying a remote user will fail.
- SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it.

### EXAMPLE

```
Console(config)#snmp-server user steve group r&d v3 auth md5 greenpeace priv des56 einstien
Console(config)#snmp-server user mark group r&d remote 192.168.1.19 v3 auth md5 greenpeace priv
  des56 einstien
Console(config)#
```

## snmp-server view

This command adds an SNMP view which controls user access to the MIB. Use the **no** form to remove an SNMP view.

### SYNTAX

**snmp-server view** *view-name oid-tree* {**included** | **excluded**}

**no snmp-server view** *view-name*

*view-name* - Name of an SNMP view. (Range: 1-32 characters)

*oid-tree* - Object identifier of a branch within the MIB tree. Wild cards can be used to mask a specific portion of the OID string. (Refer to the examples.)

**included** - Defines an included view.

**excluded** - Defines an excluded view.

### DEFAULT SETTING

defaultview (includes access to the entire MIB tree)

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- Views are used in the snmp-server group command to restrict user access to specified portions of the MIB tree.
- The predefined view "defaultview" includes access to the entire MIB tree.

### EXAMPLES

This view includes MIB-2.

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included
Console(config)#
```

This view includes the MIB-2 interfaces table, ifDescr. The wild card is used to select all the index values in this table.

```
Console(config)#snmp-server view ifEntry.2 1.3.6.1.2.1.2.2.1.*.2 included
Console(config)#
```

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

```
Console(config)#snmp-server view ifEntry.a 1.3.6.1.2.1.2.2.1.1.* included
Console(config)#
```

## show snmp engine-id

This command shows the SNMP engine ID.

### COMMAND MODE

Privileged Exec

### EXAMPLE

This example shows the default engine ID.

```
Console#show snmp engine-id
Local SNMP EngineID: 8000002a8000000000e8666672
Local SNMP EngineBoots: 1

Remote SNMP EngineID                        IP address
80000000030004e2b316c54321                     192.168.1.19
Console#
```

**Table 2: show snmp engine-id** - display description

| Field | Description |
|---|---|
| Local SNMP engineID | String identifying the engine ID. |
| Local SNMP engineBoots | The number of times that the engine has (re-)initialized since the snmp EngineID was last configured. |
| Remote SNMP engineID | String identifying an engine ID on a remote device. |
| IP address | IP address of the device containing the corresponding remote SNMP engine. |

**show snmp group** Four default groups are provided – SNMPv1 read-only access and read/write access, and SNMPv2c read-only access and read/write access.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show snmp group
Group Name     : r&d
Security Model : v3
Read View      : defaultview
Write View     : daily
Notify View    : defaultview
Storage Type   : nonvolatile
Row Status     : active

Group Name     : public
Security Model : v1
Read View      : defaultview
Write View     : No writeview specified
Notify View    : No notifyview specified
Storage Type   : volatile
Row Status     : active

Group Name     : public
Security Model : v2c
Read View      : defaultview
Write View     : No writeview specified
Notify View    : No notifyview specified
Storage Type   : volatile
Row Status     : active

Group Name     : private
Security Model : v1
Read View      : defaultview
Write View     : defaultview
Notify View    : No notifyview specified
Storage Type   : volatile
Row Status     : active

Group Name     : private
Security Model : v2c
Read View      : defaultview
Write View     : defaultview
Notify View    : No notifyview specified
Storage Type   : volatile
Row Status     : active

Console#
```

**Table 3: show snmp group** - display description

| Field | Description |
|---|---|
| Group Name | Name of an SNMP group. |
| Security Model | The SNMP version. |
| Read View | The associated read view. |
| Write View | The associated write view. |

**Table 3: show snmp group** - display description (Continued)

| Field | Description |
|---|---|
| Notify View | The associated notify view. |
| Storage Type | The storage type for this entry. |
| Row Status | The row status of this entry. |

## show snmp user

This command shows information on SNMP users.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show snmp user
EngineId: 800000ca030030f1df9ca00000
User Name: steve
Authentication Protocol: md5
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

SNMP remote user
EngineId: 80000000030004e2b316c54321
User Name: mark
Authentication Protocol: mdt
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

Console#
```

**Table 4: show snmp user** - display description

| Field | Description |
|---|---|
| EngineId | String identifying the engine ID. |
| User Name | Name of user connecting to the SNMP agent. |
| Authentication Protocol | The authentication protocol used with SNMPv3. |
| Privacy Protocol | The privacy protocol used with SNMPv3. |
| Storage Type | The storage type for this entry. |
| Row Status | The row status of this entry. |
| SNMP remote user | A user associated with an SNMP engine on a remote device. |

## show snmp view

This command shows information on the SNMP views.

**COMMAND MODE**
Privileged Exec

**EXAMPLE**

```
Console#show snmp view
View Name    : mib-2
Subtree OID  : 1.2.2.3.6.2.1
View Type    : included
Storage Type : nonvolatile
Row Status   : active

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

Console#
```

**Table 5: show snmp view** - display description

| Field | Description |
|---|---|
| View Name | Name of an SNMP view. |
| Subtree OID | A branch in the MIB tree. |
| View Type | Indicates if the view is included or excluded. |
| Storage Type | The storage type for this entry. |
| Row Status | The row status of this entry. |

## nlm

This command enables or disables the specified notification log.

**SYNTAX**

[**no**] **nlm** *filter-name*

*filter-name* - Notification log name. (Range: 1-32 characters)

**DEFAULT SETTING**
Enabled

**COMMAND MODE**
Global Configuration

**COMMAND USAGE**
- Notification logging is enabled by default, but will not start recording information until a logging profile specified by the snmp-server notify-filter command is enabled by the **nlm** command.
- Disabling logging with this command does not delete the entries stored in the notification log.

### EXAMPLE

This example enables the notification log A1.

```
Console(config)#nlm A1
Console(config)#
```

## snmp-server notify-filter

This command creates an SNMP notification log. Use the **no** form to remove this log.

### SYNTAX

[**no**] **snmp-server notify-filter** *profile-name* **remote** *ip-address*

*profile-name* - Notification log profile name. (Range: 1-32 characters)

*ip-address* - The Internet address of a remote device. The specified target host must already have been configured using the snmp-server host command.

---

**NOTE:** The notification log is stored locally. It is not sent to a remote device. This remote host parameter is only required to complete mandatory fields in the SNMP Notification MIB.

---

### DEFAULT SETTING

None

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- Systems that support SNMP often need a mechanism for recording Notification information as a hedge against lost notifications, whether those are Traps or Informs that exceed retransmission limits. The Notification Log MIB (NLM, RFC 3014) provides an infrastructure in which information from other MIBs may be logged.
- Given the service provided by the NLM, individual MIBs can now bear less responsibility to record transient information associated with an event against the possibility that the Notification message is lost, and applications can poll the log to verify that they have not missed any important Notifications.
- If notification logging is not configured and enabled, when the switch reboots, some SNMP traps (such as warm start) cannot be logged.
- To avoid this problem, notification logging should be configured and enabled using the **snmp-server notify-filter** command and nlm command, and these commands stored in the startup configuration file. Then when the switch reboots, SNMP traps (such as warm start) can now be logged.
- When this command is executed, a notification log is created (with the default parameters defined in RFC 3014). Notification logging is enabled by default (see the nlm command), but will not start recording information until a logging profile specified with this command is enabled with the nlm command.
- Based on the default settings used in RFC 3014, a notification log can contain up to 256 entries, and the entry aging time is 1440 minutes. Information recorded in a

notification log, and the entry aging time can only be configured using SNMP from a network management station.

- When a trap host is created with the snmp-server host command, a default notify filter will be created as shown in the example under the show snmp notify-filter command.

### EXAMPLE

This example first creates an entry for a remote host, and then instructs the switch to record this device as the remote host for the specified notification log.

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#snmp-server notify-filter A1 remote 10.1.19.23
Console(config)
```

## show nlm oper-status

This command shows the operational status of configured notification logs.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show nlm oper-status
Filter Name: A1
Oper-Status: Operational
Console#
```

## show snmp notify-filter

This command displays the configured notification logs.

### COMMAND MODE

Privileged Exec

### EXAMPLE

This example displays the configured notification logs and associated target hosts.

```
Console#show snmp notify-filter
Filter profile name          IP address
---------------------------- ----------------
A1                           10.1.19.23
Console#
```

# 27 REMOTE MONITORING COMMANDS

Remote Monitoring allows a remote device to collect information or respond to specified events on an independent basis. This switch is an RMON-capable device which can independently perform a wide range of tasks, significantly reducing network management traffic. It can continuously run diagnostics and log information on network performance. If an event is triggered, it can automatically notify the network administrator of a failure and provide historical information about the event. If it cannot connect to the management agent, it will continue to perform any specified tasks and pass data back to the management station the next time it is contacted.

This switch supports mini-RMON, which consists of the Statistics, History, Event and Alarm groups. When RMON is enabled, the system gradually builds up information about its physical interfaces, storing this information in the relevant RMON database group. A management agent then periodically communicates with the switch using the SNMP protocol. However, if the switch encounters a critical event, it can automatically send a trap message to the management agent which can then respond to the event if so configured.

**Table 1: RMON Commands**

| Command | Function | Mode |
|---|---|---|
| rmon alarm | Sets threshold bounds for a monitored variable | GC |
| rmon event | Creates a response event for an alarm | GC |
| rmon collection history | Periodically samples statistics | IC |
| rmon collection rmon1 | Enables statistics collection | IC |
| show rmon alarms | Shows the settings for all configured alarms | PE |
| show rmon events | Shows the settings for all configured events | PE |
| show rmon history | Shows the sampling parameters for each entry | PE |
| show rmon statistics | Shows the collected statistics | PE |

## rmon alarm

This command sets threshold bounds for a monitored variable. Use the **no** form to remove an alarm.

### SYNTAX

**rmon alarm** *index variable interval* {**absolute | delta**}
**rising-threshold** *threshold* [*event-index*] **falling-threshold** *threshold* [*event-index*]
[**owner** *name*]

**no rmon alarm** *index*

*index* – Index to this entry. (Range: 1-65535)

*variable* – The object identifier of the MIB variable to be sampled. Only variables of the type etherStatsEntry.n.n may be sampled. Note that etherStatsEntry.n uniquely defines the MIB variable, and etherStatsEntry.n.n defines the MIB variable, plus the etherStatsIndex. For example, 1.3.6.1.2.1.16.1.1.1.6.1 denotes etherStatsBroadcastPkts, plus the etherStatsIndex of 1.

*interval* – The polling interval. (Range: 1-31622400 seconds)

**absolute** – The variable is compared directly to the thresholds at the end of the sampling period.

**delta** – The last sample is subtracted from the current value and the difference is then compared to the thresholds.

*threshold* – An alarm threshold for the sampled variable.
(Range: 0-2147483647)

*event-index* – The index of the event to use if an alarm is triggered. If there is no corresponding entry in the event control table, then no event will be generated. (Range: 1-65535)

*name* – Name of the person who created this entry. (Range: 1-127 characters)

### DEFAULT SETTING

1.3.6.1.2.1.16.1.1.1.6.1 - 1.3.6.1.2.1.16.1.1.1.6.26/50
Taking delta samples every 30 seconds,
Rising threshold is 892800, assigned to event 0
Falling threshold is 446400, assigned to event 0

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- If an event is already defined for an index, the entry must be deleted before any changes can be made with this command.

- If the current value is greater than or equal to the rising threshold, and the last sample value was less than this threshold, then an alarm will be generated. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the rising threshold, reaches the falling threshold, and again moves back up to the rising threshold.

- If the current value is less than or equal to the falling threshold, and the last sample value was greater than this threshold, then an alarm will be generated. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the falling threshold, reaches the rising threshold, and again moves back down to the failing threshold.

### EXAMPLE

```
Console(config)#rmon alarm 1 1.3.6.1.2.1.16.1.1.1.6.1 15 delta
  rising-threshold 100 1 falling-threshold 30 1 owner mike
Console(config)#
```

## rmon event

This command creates a response event for an alarm. Use the **no** form to remove an event.

### SYNTAX

**rmon event** *index* [**log**] | [**trap** *community*] | [**description** *string*] | [**owner** *name*]

**no rmon event** *index*

*index* – Index to this entry. (Range: 1-65535)

**log** – Generates an RMON log entry when the event is triggered. Log messages are processed based on the current configuration settings for event logging (see "Event Logging" on page 640).

**trap** – Sends a trap message to all configured trap managers (see "snmp-server host" on page 664).

*community* – A password-like community string sent with the trap operation to SNMP v1 and v2c hosts. Although this string can be set using the **rmon event** command by itself, it is recommended that the string be defined using the snmp-server community command prior to using the rmon event command. (Range: 1-32 characters)

*string* – A comment that describes this event. (Range: 1-127 characters)

*name* – Name of the person who created this entry.
(Range: 1-127 characters)

### DEFAULT SETTING

None

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- If an event is already defined for an index, the entry must be deleted before any changes can be made with this command.

- The specified events determine the action to take when an alarm triggers this event. The response to an alarm can include logging the alarm or sending a message to a trap manager.

### EXAMPLE

```
Console(config)#rmon event 2 log description urgent owner mike
Console(config)#
```

## rmon collection history

This command periodically samples statistics on a physical interface. Use the no form to disable periodic sampling.

### SYNTAX

**rmon collection history controlEntry** *index*
[[**owner** *name*] [**buckets** *number*] [**interval** *seconds*]] |
[**buckets** *number*] [**interval** *seconds*] | **interval** *seconds*

**no rmon collection history controlEntry** *index*

*index* – Index to this entry. (Range: 1-65535)

*number* – The number of buckets requested for this entry. (Range: 1-65536)

*seconds* – The polling interval. (Range: 1-3600 seconds)

*name* – Name of the person who created this entry.
(Range: 1-127 characters)

### DEFAULT SETTING

1.3.6.1.2.1.16.1.1.1.6.1 - 1.3.6.1.2.1.16.1.1.1.6.26/50
Buckets: 8
Interval: 30 seconds for even numbered entries,
1800 seconds for odd numbered entries

### COMMAND MODE

Interface Configuration (Ethernet)

### COMMAND USAGE

- By default, each index number equates to a port on the switch, but can be changed to any number not currently in use.

- If periodic sampling is already enabled on an interface, the entry must be deleted before any changes can be made with this command.

- The information collected for each sample includes:

  input octets, packets, broadcast packets, multicast packets, undersize packets, oversize packets, fragments, jabbers, CRC alignment errors, collisions, drop events, and network utilization.

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#rmon collection history 21 buckets 24 interval 60 owner mike
Console(config-if)#
```

## rmon collection rmon1

This command enables the collection of statistics on a physical interface. Use the no form to disable statistics collection.

### SYNTAX

**rmon collection rmon1 controlEntry** *index* [**owner** *name*]

**no rmon collection rmon1 controlEntry** *index*

*index* – Index to this entry. (Range: 1-65535)

*name* – Name of the person who created this entry. (Range: 1-127 characters)

### DEFAULT SETTING

Enabled

### COMMAND MODE

Interface Configuration (Ethernet)

### COMMAND USAGE

- By default, each index number equates to a port on the switch, but can be changed to any number not currently in use.
- If statistics collection is already enabled on an interface, the entry must be deleted before any changes can be made with this command.
- The information collected for each entry includes:

  input octets, packets, broadcast packets, multicast packets, undersize packets, oversize packets, fragments, jabbers, CRC alignment errors, collisions, drop events, and packets of specified lengths

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#rmon collection rmon1 controlEntry 1 owner mike
Console(config-if)#
```

## show rmon alarms

This command shows the settings for all configured alarms.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show rmon alarms
Alarm 1 is valid, owned by
 Monitors 1.3.6.1.2.1.16.1.1.1.6.1 every 30 seconds
 Taking delta samples, last value was 0
 Rising threshold is 892800, assigned to event 0
 Falling threshold is 446400, assigned to event 0
:
```

## show rmon events

This command shows the settings for all configured events.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show rmon events
Event 2 is valid, owned by mike
 Description is urgent
 Event firing causes log and trap to community , last fired  00:00:00
Console#
```

## show rmon history

This command shows the sampling parameters configured for each entry in the history group.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show rmon history
Entry 1 is valid, and owned by
 Monitors 1.3.6.1.2.1.2.2.1.1.1 every 1800 seconds
 Requested # of time intervals, ie buckets, is 8
 Granted # of time intervals, ie buckets, is 8
  Sample # 1 began measuring at 00:00:01
  Received 77671 octets, 1077 packets,
  61 broadcast and 978 multicast packets,
  0 undersized and 0 oversized packets,
  0 fragments and 0 jabbers packets,
  0 CRC alignment errors and 0 collisions.
  # of dropped packet events is 0
  Network utilization is estimated at 0
:
```

## show rmon statistics

This command shows the information collected for all configured entries in the statistics group.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show rmon statistics
Interface 1 is valid, and owned by
 Monitors 1.3.6.1.2.1.2.2.1.1.1 which has
 Received 164289 octets, 2372 packets,
 120 broadcast and 2211 multicast packets,
 0 undersized and 0 oversized packets,
 0 fragments and 0 jabbers,
 0 CRC alignment errors and 0 collisions.
 # of dropped packet events (due to lack of resources): 0
```

```
# of packets received of length (in octets):
 64: 2245, 65-127: 87, 128-255: 31,
 256-511: 5, 512-1023: 2, 1024-1518: 2
:
```

# 28 FLOW SAMPLING COMMANDS

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

**Table 1: sFlow Commands**

| Command | Function | Mode |
|---|---|---|
| sflow destination | Configures the IP address and UDP port used by the Collector | IC |
| sflow max-datagram-size | Configures the maximum size of the sFlow datagram payload | IC |
| sflow max-header-size | Configures the maximum size of the sFlow datagram header | IC |
| sflow owner | Configures the name of the receiver | IC |
| sflow sample | Configures the packet sampling rate | IC |
| sflow source | Enables sFlow on the source ports to be monitored | IC |
| sflow timeout | Configures the length of time samples are sent to the Collector before resetting all sFlow port parameters | IC |
| show sflow | Shows the global and interface settings for the sFlow process | PE |

## sflow destination

This command configures the IP address and UDP port used by the Collector. Use the **no** form to restore the default settings.

### SYNTAX

**sflow destination** {**ipv4** *ipv4-address* | **ipv6** *ipv6-address*} [*destination-udp-port*]

**no sflow destination**

*ipv4-address* - IPv4 address of the sFlow Collector. Valid IPv4 addresses consist of four decimal numbers, 0 to 255, separated by periods.

*ipv6-address* - IPv6 address of the sFlow Collector. A full IPv6 address including the network prefix and host address bits. An IPv6 address consists of 8 colon-separated 16-bit hexadecimal values. One double colon may be used to indicate the appropriate number of zeros required to fill the undefined fields.

*destination-udp-port* - The UDP port on which the Collector is listening for sFlow streams. (Range: 0-65534)

### DEFAULT SETTING
IP Address: null
UDP Port: 6343

### COMMAND MODE
Interface Configuration (Ethernet)

### EXAMPLE
This example configures the Collector's IP address, and uses the default UDP port.

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow destination ipv4 192.168.0.4
Console(config-if)#
```

## sflow max-datagram-size

This command configures the maximum size of the sFlow datagram payload. Use the **no** form to restore the default setting.

### SYNTAX

**sflow max-datagram-size** *max-datagram-size*

**no max-datagram-size**

*max-datagram-size* - The maximum size of the sFlow datagram payload. (Range: 200-1500 bytes)

### DEFAULT SETTING
1400 bytes

### COMMAND MODE
Interface Configuration (Ethernet)

### EXAMPLE

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow max-datagram-size 1500
Console(config-if)#
```

## sflow max-header-size

This command configures the maximum size of the sFlow datagram header. Use the **no** form to restore the default setting.

### SYNTAX

**sflow max-header-size** *max-header-size*

**no max-header-size**

*max-header-size* - The maximum size of the sFlow datagram header. (Range: 64-256 bytes)

**DEFAULT SETTING**
128 bytes

**COMMAND MODE**
Interface Configuration (Ethernet)

**EXAMPLE**

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow max-header-size 256
Console(config-if)#
```

## sflow owner

This command configures the name of the receiver (i.e., sFlow Collector). Use the **no** form to remove this name.

**SYNTAX**

**sflow owner** *name*

**no sflow owner**

*name* - The name of the receiver. (Range: 1-256 characters)

**DEFAULT SETTING**
None

**COMMAND MODE**
Interface Configuration (Ethernet)

**EXAMPLE**
This example set the owner's name to Lamar.

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow owner Lamer
Console(config-if)#
```

## sflow sample

This command configures the packet sampling rate. Use the **no** form to restore the default rate.

**SYNTAX**

**sflow sample** *rate*

**no sflow sample**

*rate* - The packet sampling rate, or the number of packets out of which one sample will be taken. (Range: 256-16777215 packets)

**DEFAULT SETTING**
Disabled

**COMMAND MODE**
Interface Configuration (Ethernet)

**EXAMPLE**
This example sets the sample rate to 1 out of every 100 packets.

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow sample 100
Console(config-if)#
```

## sflow source

This command enables sFlow on the source ports to be monitored. Use the **no** form to disable sFlow on the specified ports.

**SYNTAX**

[**no**] **sflow source**

**DEFAULT SETTING**
Disabled

**COMMAND MODE**
Interface Configuration (Ethernet)

**EXAMPLE**
This example enables flow control on ports 9 through 16.

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow source
Console(config-if)#
```

## sflow timeout

This command configures the length of time samples are sent to the Collector before resetting all sFlow port parameters. Use the **no** form to restore the default time out.

**SYNTAX**

**sflow timeout** *seconds*

**no sflow timeout**

*seconds* - The length of time the sFlow process continuously sends samples to the Collector before resetting all sFlow port parameters. (Range: 0-10000000 seconds, where 0 indicates no time out)

**DEFAULT SETTING**
Disabled

**COMMAND MODE**
Interface Configuration (Ethernet)

#### COMMAND USAGE

The sFlow parameters affected by this command include the sampling interval, the receiver's name, address and UDP port, the time out, maximum header size, and maximum datagram size.

#### EXAMPLE

This example sets the time out to 1000 seconds.

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow timeout 10000
Console(config-if)#
```

### show sflow

This command shows the global and interface settings for the sFlow process.

#### SYNTAX

**show sflow interface** [*interface*]

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

#### COMMAND MODE

Privileged Exec

#### EXAMPLE

```
Console#show sflow interface ethernet 1/9

 Interface of Ethernet  1/9  :
   Interface status      : Enabled
   Owner name            : Lamar
   Owner destination     : 192.168.0.4
   Owner socket port     : 6343
   Time out              : 9994
   Maximum header size   : 256
   Maximum datagram size : 1500
   Sample rate           : 1/256

Console#
```

# 29 AUTHENTICATION COMMANDS

You can configure this switch to authenticate users logging into the system for management access using local or remote authentication methods. Port-based authentication using IEEE 802.1X can also be configured to control either management access to the uplink ports or client access[1] to the data ports.

**Table 1: Authentication Commands**

| Command Group | Function |
|---|---|
| User Accounts | Configures the basic user names and passwords for management access |
| Authentication Sequence | Defines logon authentication method and precedence |
| RADIUS Client | Configures settings for authentication via a RADIUS server |
| TACACS+ Client | Configures settings for authentication via a TACACS+ server |
| AAA | Configures authentication, authorization, and accounting for network access |
| Web Server | Enables management access via a web browser |
| Telnet Server | Enables management access via Telnet |
| Secure Shell | Provides secure replacement for Telnet |
| 802.1X Port Authentication | Configures host authentication on specific ports using 802.1X |
| Management IP Filter | Configures IP addresses that are allowed management access |

## USER ACCOUNTS

The basic commands required for management access are listed in this section. This switch also includes other options for password checking via the console or a Telnet connection (page 630), user authentication via a remote authentication server (page 691), and host access authentication for specific ports (page 725).

**Table 2: User Access Commands**

| Command | Function | Mode |
|---|---|---|
| enable password | Sets a password to control access to the Privileged Exec level | GC |
| username | Establishes a user name-based authentication system at login | GC |

1. For other methods of controlling client access, see "General Security Measures" on page 739.

## enable password

After initially logging onto the system, you should set the Privileged Exec password. Remember to record it in a safe place. This command controls access to the Privileged Exec level from the Normal Exec level. Use the **no** form to reset the default password.

### SYNTAX

**enable password** [**level** *level*] {**0** | **7**} *password*

**no enable password** [**level** *level*]

**level** *level* - Level 15 for Privileged Exec. (Levels 0-14 are not used.)

{**0** | **7**} - 0 means plain password, 7 means encrypted password.

*password* - password for this privilege level. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

### DEFAULT SETTING

The default is level 15.
The default password is “super”

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- You cannot set a null password. You will have to enter a password to change the command mode from Normal Exec to Privileged Exec with the enable command.
- The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

### EXAMPLE

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

### RELATED COMMANDS

enable (609)
authentication enable (694)

## 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 3: Default Login Settings**

| username | access-level | password |
|---|---|---|
| guest | 0 | guest |
| admin | 15 | admin |

### COMMAND MODE

Global Configuration

### COMMAND USAGE

The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from an FTP/TFTP server. There is no need for you to manually configure encrypted passwords.

### EXAMPLE

This example shows how the set the access level and password for a user.

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

## AUTHENTICATION SEQUENCE

Three authentication methods can be specified to authenticate users logging into the system for management access. The commands in this section can be used to define the authentication method and sequence.

**Table 4: Authentication Sequence Commands**

| Command | Function | Mode |
|---|---|---|
| authentication enable | Defines the authentication method and precedence for command mode change | GC |
| authentication login | Defines logon authentication method and precedence | GC |

## authentication enable

This command defines the authentication method and precedence to use when changing from Exec command mode to Privileged Exec command mode with the enable command. Use the **no** form to restore the default.

### SYNTAX

**authentication enable** {[**local**] [**radius**] [**tacacs**]}

**no authentication enable**

**local** - Use local password only.

**radius** - Use RADIUS server password only.

**tacacs** - Use TACACS server password.

### DEFAULT SETTING

Local

### COMMAND MODE

Global Configuration

### COMMAND USAGE

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

- RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.

- You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter "**authentication enable radius tacacs local**," the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

### EXAMPLE

```
Console(config)#authentication enable radius
Console(config)#
```

### RELATED COMMANDS

enable password - sets the password for changing command modes (692)

## authentication login

This command defines the login authentication method and precedence. Use the **no** form to restore the default.

### SYNTAX

**authentication login** {[**local**] [**radius**] [**tacacs**]}

**no authentication login**

**local** - Use local password.

**radius** - Use RADIUS server password.

**tacacs** - Use TACACS server password.

### DEFAULT SETTING

Local

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.
- RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter "**authentication login radius tacacs local**," the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

### EXAMPLE

```
Console(config)#authentication login radius
Console(config)#
```

### RELATED COMMANDS

username - for setting the local user names and passwords (692)

## RADIUS CLIENT

Remote Authentication Dial-in User Service (RADIUS) is a logon authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

**Table 5: RADIUS Client Commands**

| Command | Function | Mode |
|---|---|---|
| radius-server acct-port | Sets the RADIUS server network port | GC |
| radius-server auth-port | Sets the RADIUS server network port | GC |

**Table 5: RADIUS Client Commands**

| Command | Function | Mode |
|---|---|---|
| radius-server host | Specifies the RADIUS server | GC |
| radius-server key | Sets the RADIUS encryption key | GC |
| radius-server retransmit | Sets the number of retries | GC |
| radius-server timeout | Sets the interval between sending authentication requests | GC |
| show radius-server | Shows the current RADIUS settings | PE |

## radius-server acct-port

This command sets the RADIUS server network port for accounting messages. Use the **no** form to restore the default.

### SYNTAX

**radius-server acct-port** *port-number*

**no radius-server acct-port**

*port-number* - RADIUS server UDP port used for accounting messages. (Range: 1-65535)

### DEFAULT SETTING

1813

### COMMAND MODE

Global Configuration

### EXAMPLE

```
Console(config)#radius-server acct-port 181
Console(config)#
```

## radius-server auth-port

This command sets the RADIUS server network port. Use the **no** form to restore the default.

### SYNTAX

**radius-server auth-port** *port-number*

**no radius-server auth-port**

*port-number* - RADIUS server UDP port used for authentication messages. (Range: 1-65535)

### DEFAULT SETTING

1812

### COMMAND MODE

Global Configuration

### EXAMPLE

```
Console(config)#radius-server auth-port 181
Console(config)#
```

## radius-server host

This command specifies primary and backup RADIUS servers, and authentication and accounting parameters that apply to each server. Use the **no** form to remove a specified server, or to restore the default values.

### SYNTAX

[**no**] **radius-server** *index* **host** *host-ip-address* [**auth-port** *auth-port*] [**acct-port** *acct_port*] [**key** *key*] [**retransmit** *retransmit*] [**timeout** *timeout*]

*index* - Allows you to specify up to five servers. These servers are queried in sequence until a server responds or the retransmit period expires.

*host-ip-address* - IP address of server.

*auth-port* - RADIUS server UDP port used for authentication messages. (Range: 1-65535)

*acct_port* - RADIUS server UDP port used for accounting messages. (Range: 1-65535)

*key* - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)

*retransmit* - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1-30)

*timeout* - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

### DEFAULT SETTING

**auth-port** - 1812
**acct-port** - 1813
**timeout** - 5 seconds
**retransmit** - 2

### COMMAND MODE

Global Configuration

### EXAMPLE

```
Console(config)#radius-server 1 host 192.168.1.20 port 181 timeout 10 retransmit 5 key green
Console(config)#
```

## radius-server key

This command sets the RADIUS encryption key. Use the **no** form to restore the default.

### SYNTAX

**radius-server key** *key-string*

**no radius-server key**

*key-string* - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)

### DEFAULT SETTING

None

### COMMAND MODE

Global Configuration

### EXAMPLE

```
Console(config)#radius-server key green
Console(config)#
```

## radius-server retransmit

This command sets the number of retries. Use the **no** form to restore the default.

### SYNTAX

**radius-server retransmit** *number-of-retries*

**no radius-server retransmit**

*number-of-retries* - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1 - 30)

### DEFAULT SETTING

2

### COMMAND MODE

Global Configuration

### EXAMPLE

```
Console(config)#radius-server retransmit 5
Console(config)#
```

## radius-server timeout

This command sets the interval between transmitting authentication requests to the RADIUS server. Use the **no** form to restore the default.

### SYNTAX

**radius-server timeout** *number-of-seconds*

**no radius-server timeout**

*number-of-seconds* - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

#### DEFAULT SETTING

5

#### COMMAND MODE

Global Configuration

#### EXAMPLE

```
Console(config)#radius-server timeout 10
Console(config)#
```

## show radius-server

This command displays the current settings for the RADIUS server.

#### DEFAULT SETTING

None

#### COMMAND MODE

Privileged Exec

#### EXAMPLE

```
Console#show radius-server

Remote RADIUS Server Configuration:

Global Settings:
 Authentication Port Number : 1812
 Accounting Port Number     : 1813
 Retransmit Times           : 2
 Request Timeout            : 5

Server 1:
 Server IP Address   : 192.168.1.1
 Auth-port           : 1812
 Acct-port           : 1813
 Retransmit Times    : 2
 Request Timeout     : 5

Radius Server Group:
Group Name                Member Index
------------------------- -------------
radius                    1

Console#
```

# TACACS+ CLIENT

Terminal Access Controller Access Control System (TACACS+) is a logon authentication protocol that uses software running on a central server to control access to TACACS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

**Table 6: TACACS+ Client Commands**

| Command | Function | Mode |
|---|---|---|
| tacacs-server | Specifies the TACACS+ server and optional parameters | GC |
| tacacs-server host | Specifies the TACACS+ server | GC |
| tacacs-server key | Sets the TACACS+ encryption key | GC |
| tacacs-server port | Specifies the TACACS+ server network port | GC |
| show tacacs-server | Shows the current TACACS+ settings | GC |

## tacacs-server

This command specifies the TACACS+ server and other optional parameters. Use the **no** form to remove the server, or to restore the default values.

### SYNTAX

**tacacs-server** *index* **host** *host-ip-address* [**key** *key*] [**port** *port-number*]

**no tacacs-server** *index*

*index* - The index for this server. (Range: 1)

*host-ip-address* - IP address of a TACACS+ server.

*key* - Encryption key used to authenticate logon access for the client. Do not use blank spaces in the string. (Maximum length: 48 characters)

*port-number* - TACACS+ server TCP port used for authentication messages. (Range: 1-65535)

### DEFAULT SETTING

10.11.12.13

### COMMAND MODE

Global Configuration

### EXAMPLE

```
Console(config)#tacacs-server host 192.168.1.25
Console(config)#
```

## tacacs-server host

This command specifies the TACACS+ server. Use the **no** form to restore the default.

### SYNTAX

**tacacs-server host** *host-ip-address*

**no tacacs-server host**

*host-ip-address* - IP address of a TACACS+ server.

### DEFAULT SETTING

10.11.12.13

### COMMAND MODE

Global Configuration

### EXAMPLE

```
Console(config)#tacacs-server host 192.168.1.25
Console(config)#
```

## tacacs-server key

This command sets the TACACS+ encryption key. Use the **no** form to restore the default.

### SYNTAX

**tacacs-server key** *key-string*

**no tacacs-server key**

*key-string* - Encryption key used to authenticate logon access for the client. Do not use blank spaces in the string.
(Maximum length: 48 characters)

### DEFAULT SETTING

None

### COMMAND MODE

Global Configuration

### EXAMPLE

```
Console(config)#tacacs-server key green
Console(config)#
```

## tacacs-server port

This command specifies the TACACS+ server network port. Use the **no** form to restore the default.

### SYNTAX

**tacacs-server port** *port-number*

**no tacacs-server port**

*port-number* - TACACS+ server TCP port used for authentication messages. (Range: 1-65535)

### DEFAULT SETTING
49

### COMMAND MODE
Global Configuration

### EXAMPLE

```
Console(config)#tacacs-server port 181
Console(config)#
```

## show tacacs-server

This command displays the current settings for the TACACS+ server.

### DEFAULT SETTING
None

### COMMAND MODE
Privileged Exec

### EXAMPLE

```
Console#show tacacs-server

Remote TACACS+ Server Configuration:

Global Settings:
 Server Port Number: 49

Server 1:
 Server IP Address  : 10.11.12.13
 Server Port Number : 49

Tacacs Server Group:
Group Name               Member Index
------------------------ -------------
tacacs+                  1
Console#
```

# AAA

The Authentication, Authorization, and Accounting (AAA) feature provides the main framework for configuring access control on the switch. The AAA functions require the use of configured RADIUS or TACACS+ servers in the network.

**Table 7: AAA Commands**

| Command | Function | Mode |
|---|---|---|
| aaa accounting commands | Enables accounting of Exec mode commands | GC |
| aaa accounting dot1x | Enables accounting of 802.1X services | GC |
| aaa accounting exec | Enables accounting of Exec services | GC |
| aaa accounting update | Enables periodoc updates to be sent to the accounting server | GC |
| aaa authorization exec | Enables authorization of Exec sessions | GC |
| aaa group server | Groups security servers in to defined lists | GC |
| server | Configures the IP address of a server in a group list | SG |
| accounting dot1x | Applies an accounting method to an interface for 802.1X service requests | IC |
| accounting exec | Applies an accounting method to local console, Telnet or SSH connections | Line |
| authorization exec | Applies an authorization method to local console, Telnet or SSH connections | Line |
| show accounting | Displays all accounting information | PE |

## aaa accounting commands

This command enables the accounting of Exec mode commands. Use the **no** form to disable the accounting service.

### SYNTAX

**aaa accounting commands** *level* {**default** | *method-name*} **start-stop group** {**tacacs+** |*server-group*}

**no aaa accounting commands** *level* {**default** | *method-name*}

*level* - The privilege level for executing commands. (Range: 0-15)

**default** - Specifies the default accounting method for service requests.

*method-name* - Specifies an accounting method for service requests. (Range: 1-255 characters)

**start-stop** - Records accounting from starting point and stopping point.

**group** - Specifies the server group to use.

**tacacs+** - Specifies all TACACS+ hosts configure with the tacacs-server host command.

*server-group* - Specifies the name of a server group configured with the aaa group server command. (Range: 1-255 characters)

**DEFAULT SETTING**
Accounting is not enabled
No servers are specified

**COMMAND MODE**
Global Configuration

**COMMAND USAGE**
■The accounting of Exec mode commands is only supported by TACACS+ servers.

■Note that the **default** and *method-name* fields are only used to describe the accounting method(s) configured on the specified TACACS+ server, and do not actually send any information to the server about the methods to use.

**EXAMPLE**

```
Console(config)#aaa accounting commands 15 default start-stop group tacacs+
Console(config)#
```

## aaa accounting dot1x

This command enables the accounting of requested 802.1X services for network access. Use the **no** form to disable the accounting service.

**SYNTAX**

**aaa accounting dot1x** {**default** | *method-name*}
**start-stop group** {**radius** | **tacacs+** |*server-group*}

**no aaa accounting dot1x** {**default** | *method-name*}

**default** - Specifies the default accounting method for service requests.

*method-name* - Specifies an accounting method for service requests. (Range: 1-255 characters)

**start-stop** - Records accounting from starting point and stopping point.

**group** - Specifies the server group to use.

**radius** - Specifies all RADIUS hosts configure with the radius-server host command.

**tacacs+** - Specifies all TACACS+ hosts configure with the tacacs-server host command.

*server-group* - Specifies the name of a server group configured with the aaa group server command. (Range: 1-255 characters)

**DEFAULT SETTING**
Accounting is not enabled
No servers are specified

**COMMAND MODE**
Global Configuration

#### COMMAND USAGE

Note that the **default** and *method-name* fields are only used to describe the accounting method(s) configured on the specified RADIUS or TACACS+ servers, and do not actually send any information to the servers about the methods to use.

#### EXAMPLE

```
Console(config)#aaa accounting dot1x default start-stop group radius
Console(config)#
```

### aaa accounting exec

This command enables the accounting of requested Exec services for network access. Use the **no** form to disable the accounting service.

#### SYNTAX

**aaa accounting exec** {**default** | *method-name*}
**start-stop group** {**radius** | **tacacs+** |*server-group*}

**no aaa accounting exec** {**default** | *method-name*}

**default** - Specifies the default accounting method for service requests.

*method-name* - Specifies an accounting method for service requests. (Range: 1-255 characters)

**start-stop** - Records accounting from starting point and stopping point.

**group** - Specifies the server group to use.

**radius** - Specifies all RADIUS hosts configure with the radius-server host command.

**tacacs+** - Specifies all TACACS+ hosts configure with the tacacs-server host command.

*server-group* - Specifies the name of a server group configured with the aaa group server command. (Range: 1-255 characters)

#### DEFAULT SETTING

Accounting is not enabled
No servers are specified

#### COMMAND MODE

Global Configuration

#### COMMAND USAGE

- This command runs accounting for Exec service requests for the local console and Telnet connections.
- Note that the **default** and *method-name* fields are only used to describe the accounting method(s) configured on the specified RADIUS or TACACS+ servers, and do not actually send any information to the servers about the methods to use.

### EXAMPLE

```
Console(config)#aaa accounting exec default start-stop group tacacs+
Console(config)#
```

## aaa accounting update

This command enables the sending of periodic updates to the accounting server. Use the **no** form to disable accounting updates.

### SYNTAX

**aaa accounting update** [**periodic** *interval*]

**no aaa accounting update**

*interval* - Sends an interim accounting record to the server at this interval. (Range: 1-2147483647 minutes)

### DEFAULT SETTING

1 minute

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- When accounting updates are enabled, the switch issues periodic interim accounting records for all users on the system.
- Using the command without specifying an interim interval enables updates, but does not change the current interval setting.

### EXAMPLE

```
Console(config)#aaa accounting update periodic 30
Console(config)#
```

## aaa authorization exec

This command enables the authorization for Exec access. Use the **no** form to disable the authorization service.

### SYNTAX

**aaa authorization exec** {**default** | *method-name*}
**group** {**tacacs+** | *server-group*}

**no aaa authorization exec** {**default** | *method-name*}

**default** - Specifies the default authorization method for Exec access.

*method-name* - Specifies an authorization method for Exec access. (Range: 1-255 characters)

**group** - Specifies the server group to use.

**tacacs+** - Specifies all TACACS+ hosts configured with the tacacs-server command.

*server-group* - Specifies the name of a server group configured with the aaa group server command. (Range: 1-255 characters)

### DEFAULT SETTING

Authorization is not enabled
No servers are specified

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- This command performs authorization to determine if a user is allowed to run an Exec shell.
- AAA authentication must be enabled before authorization is enabled.
- If this command is issued without a specified named method, the default method list is applied to all interfaces or lines (where this authorization type applies), except those that have a named method explicitly defined.

### EXAMPLE

```
Console(config)#aaa authorization exec default group tacacs+
Console(config)#
```

## aaa group server

Use this command to name a group of security server hosts. To remove a server group from the configuration list, enter the **no** form of this command.

### SYNTAX

[**no**] **aaa group server** {**radius** | **tacacs+**} *group-name*

**radius** - Defines a RADIUS server group.

**tacacs+** - Defines a TACACS+ server group.

*group-name* - A text string that names a security server group. (Range: 1-7 characters)

### DEFAULT SETTING

None

### COMMAND MODE

Global Configuration

#### EXAMPLE

```
Console(config)#aaa group server radius tps
Console(config-sg-radius)#
```

### server

This command adds a security server to an AAA server group. Use the **no** form to remove the associated server from the group.

#### SYNTAX

[**no**] **server** {*index* | *ip-address*}

*index* - Specifies the server index.
(Range: RADIUS 1-5, TACACS+ 1)

*ip-address* - Specifies the host IP address of a server.

#### DEFAULT SETTING

None

#### COMMAND MODE

Server Group Configuration

#### COMMAND USAGE

- When specifying the index for a RADIUS server, that server index must already be defined by the radius-server host command.
- When specifying the index for a TACACS+ server, that server index must already be defined by the tacacs-server host command.

#### EXAMPLE

```
Console(config)#aaa group server radius tps
Console(config-sg-radius)#server 10.2.68.120
Console(config-sg-radius)#
```

### accounting dot1x

This command applies an accounting method for 802.1X service requests on an interface. Use the **no** form to disable accounting on the interface.

#### SYNTAX

**accounting dot1x** {**default** | *list-name*}

**no accounting dot1x**

**default** - Specifies the default method list created with the aaa accounting dot1x command.

*list-name* - Specifies a method list created with the aaa accounting dot1x command.

#### DEFAULT SETTING

None

### COMMAND MODE
Interface Configuration

### EXAMPLE

```
Console(config)#interface ethernet 1/2
Console(config-if)#accounting dot1x tps
Console(config-if)#
```

## accounting exec

This command applies an accounting method to local console, Telnet or SSH connections. Use the **no** form to disable accounting on the line.

### SYNTAX

**accounting exec** {**default** | *list-name*}

**no accounting exec**

**default** - Specifies the default method list created with the aaa accounting exec command.

*list-name* - Specifies a method list created with the aaa accounting exec command.

### DEFAULT SETTING
None

### COMMAND MODE
Line Configuration

### EXAMPLE

```
Console(config)#line console
Console(config-line)#accounting exec tps
Console(config-line)#exit
Console(config)#line vty
Console(config-line)#accounting exec default
Console(config-line)#
```

## authorization exec

This command applies an authorization method to local console, Telnet or SSH connections. Use the **no** form to disable authorization on the line.

### SYNTAX

**authorization exec** {**default** | *list-name*}

**no authorization exec**

**default** - Specifies the default method list created with the aaa authorization exec command.

*list-name* - Specifies a method list created with the aaa authorization exec command.

#### DEFAULT SETTING
None

#### COMMAND MODE
Line Configuration

#### EXAMPLE

```
Console(config)#line console
Console(config-line)#authorization exec tps
Console(config-line)#exit
Console(config)#line vty
Console(config-line)#authorization exec default
Console(config-line)#
```

## show accounting

This command displays the current accounting settings per function and per port.

#### SYNTAX

**show accounting** [**commands** [*level*]] |
[[**dot1x** [**statistics** [**username** *user-name* | **interface** *interface*]] | **exec** [**statistics**] | **statistics**]

**commands** - Displays command accounting information.

*level* - Displays command accounting information for a specifiable command level.

**dot1x** - Displays dot1x accounting information.

**exec** - Displays Exec accounting records.

**statistics** - Displays accounting records.

*user-name* - Displays accounting records for a specifiable username.

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-26)

#### DEFAULT SETTING
None

#### COMMAND MODE
Privileged Exec

#### EXAMPLE

```
Console#show accounting
Accounting Type : dot1x
  Method List   : default
  Group List    : radius
  Interface     : Eth 1/1
```

```
  Method List   : tps
  Group List    : radius
  Interface     : Eth 1/2

Accounting Type : EXEC
  Method List   : default
  Group List    : tacacs+
  Interface     : vty

Console#
```

## WEB SERVER

This section describes commands used to configure web browser management access to the switch.

**Table 8: Web Server Commands**

| Command | Function | Mode |
|---|---|---|
| ip http port | Specifies the port to be used by the web browser interface | GC |
| ip http server | Allows the switch to be monitored or configured from a browser | GC |
| ip http secure-server | Enables HTTPS (HTTP/SSL) for encrypted communications | GC |
| ip http secure-port | Specifies the UDP port number for HTTPS | GC |

### ip http port

This command specifies the TCP port number used by the web browser interface. Use the **no** form to use the default port.

#### SYNTAX

**ip http port** *port-number*

**no ip http port**

*port-number* - The TCP port to be used by the browser interface. (Range: 1-65535)

#### DEFAULT SETTING

80

#### COMMAND MODE

Global Configuration

#### EXAMPLE

```
Console(config)#ip http port 769
Console(config)#
```

#### RELATED COMMANDS

ip http server (712)
show system (620)

## ip http server

This command allows this device to be monitored or configured from a browser. Use the **no** form to disable this function.

### SYNTAX

[**no**] **ip http server**

### DEFAULT SETTING

Enabled

### COMMAND MODE

Global Configuration

### EXAMPLE

```
Console(config)#ip http server
Console(config)#
```

### RELATED COMMANDS

ip http port (711)
show system (620)

## ip http secure-server

This command enables the secure hypertext transfer protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's web interface. Use the **no** form to disable this function.

### SYNTAX

[**no**] **ip http secure-server**

### DEFAULT SETTING

Enabled

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- Both HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure the HTTP and HTTPS servers to use the same UDP port.

- If you enable HTTPS, you must indicate this in the URL that you specify in your browser: **https**://*device*[:*port_number*]

- When you start HTTPS, the connection is established in this way:

  - The client authenticates the server using the server's digital certificate.

  - The client and server negotiate a set of security protocols to use for the connection.

- ◆ The client and server generate session keys for encrypting and decrypting data.

- ■The client and server establish a secure encrypted connection.

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

  The following web browsers and operating systems currently support HTTPS:

**Table 9: HTTPS System Support**

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

- ■To specify a secure-site certificate, see “Replacing the Default Secure-site Certificate” on page 266. Also refer to the copy tftp https-certificate command.

### EXAMPLE

```
Console(config)#ip http secure-server
Console(config)#
```

### RELATED COMMANDS

ip http secure-port (713)
copy tftp https-certificate (625)
show system (620)

## ip http secure-port

This command specifies the UDP port number used for HTTPS connection to the switch’s web interface. Use the **no** form to restore the default port.

### SYNTAX

**ip http secure-port** *port_number*

**no ip http secure-port**

*port_number* – The UDP port used for HTTPS. (Range: 1-65535)

### DEFAULT SETTING

443

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- ■You cannot configure the HTTP and HTTPS servers to use the same port.

■ If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format: **https://***device***:***port_number*

### EXAMPLE

```
Console(config)#ip http secure-port 1000
Console(config)#
```

### RELATED COMMANDS

ip http secure-server (712)
show system (620)

## TELNET SERVER

This section describes commands used to configure Telnet management access to the switch.

**Table 10: Telnet Server Commands**

| Command | Function | Mode |
|---|---|---|
| ip telnet max-sessions | Specifies the maximum number of Telnet sessions that can simultaneously connect to this system | GC |
| ip telnet port | Specifies the port to be used by the Telnet interface | GC |
| ip telnet server | Allows the switch to be monitored or configured from Telnet | GC |
| show ip telnet | Displays configuration settings for the Telnet server | PE |

**NOTE:** This switch also supports a Telnet client function. A Telnet connection can be made from this switch to another device by entering the **telnet** command at the Privileged Exec configuration level.

### ip telnet max-sessions

This command specifies the maximum number of Telnet sessions that can simultaneously connect to this system. Use the **no** from to restore the default setting.

### SYNTAX

**ip telnet max-sessions** *session-count*

**no ip telnet max-sessions**

*session-count* - The maximum number of allowed Telnet session. (Range: 0-4)

### DEFAULT SETTING

4 sessions

#### COMMAND MODE
Global Configuration

#### COMMAND USAGE
A maximum of four sessions can be concurrently opened for Telnet and Secure Shell (i.e., both Telnet and SSH share a maximum number or four sessions).

#### EXAMPLE

```
Console(config)#ip telnet max-sessions 1
Console(config)#
```

### 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 telnet port**

*port-number* - The TCP port number 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)#
```

**show ip telnet** This command displays the configuration settings for the Telnet server.

### COMMAND MODE

Normal Exec, Privileged Exec

### EXAMPLE

```
Console#show ip telnet
IP Telnet Configuration:

Telnet Status: Enabled
Telnet Service Port: 23
Telnet Max Session: 4
Console#
```

## SECURE SHELL

This section describes the commands used to configure the SSH server. Note that you also need to install a SSH client on the management station when using this protocol to configure the switch.

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

**Table 11: Secure Shell Commands**

| Command | Function | Mode |
|---|---|---|
| ip ssh authentication-retries | Specifies the number of retries allowed by a client | GC |
| ip ssh server | Enables the SSH server on the switch | GC |
| ip ssh server-key size | Sets the SSH server key size | GC |
| ip ssh timeout | Specifies the authentication timeout for the SSH server | GC |
| copy tftp public-key | Copies the user’s public key from a TFTP server to the switch | PE |
| delete public-key | Deletes the public key for the specified user | PE |
| disconnect | Terminates a line connection | PE |
| ip ssh crypto host-key generate | Generates the host key | PE |
| ip ssh crypto zeroize | Clear the host key from RAM | PE |
| ip ssh save host-key | Saves the host key from RAM to flash memory | PE |
| show ip ssh | Displays the status of the SSH server and the configured values for authentication timeout and retries | PE |

**Table 11: Secure Shell Commands (Continued)**

| Command | Function | Mode |
|---|---|---|
| show public-key | Shows the public key for the specified user or for the host | PE |
| show ssh | Displays the status of current SSH sessions | PE |
| show users | Shows SSH users, including privilege level and public key type | PE |

*Configuration Guidelines*

The SSH server on this switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified by the authentication login command. If public key authentication is specified by the client, then you must configure authentication keys on both the client and the switch as described in the following section. Note that regardless of whether you use public key or password authentication, you still have to generate authentication keys on the switch and enable the SSH server.

To use the SSH server, complete these steps:

Generate a Host Key Pair – Use the ip ssh crypto host-key generate command to create a host public/private key pair.

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
10825913212890233765468017262725714134287629413011961955667825956641048
9574278881462065194174677298486546861571773939016477935594230357741309802
273708779454524083971752646358058176716709574804776117

Import Client’s Public Key to the Switch – Use the copy tftp public-key command to copy a file containing the public key for all the SSH client’s granted management access to the switch. (Note that these clients must be configured locally on the switch with the username command.) The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as shown in the following example for an RSA key:

1024 35
134108168560989392104094492015542534763164192187295892114317388005553616
163105177594083868631109291232226828519254374603100937187721199696317813
662774141689851320491172048303392543241016379975923714490119380060902539
484084827178194372288402533115952134861022902978982721353267131629432532
818915045306393916643 steve@192.168.1.19

Set the Optional Parameters – Set other optional parameters, including the authentication timeout, the number of retries, and the server key size.

Enable SSH Service – Use the ip ssh server command to enable the SSH server on the switch.

*Authentication* – One of the following authentication methods is employed:

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

**The client sends its password to the server.**
The switch compares the client's password to those stored in memory.
If a match is found, the connection is allowed.

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

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

*Authenticating SSH v1.5 Clients*

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

*Authenticating SSH v2 Clients*

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

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

**NOTE:** The SSH server can be accessed using any configured IPv4 or IPv6 interface address on the switch.

## ip ssh authentication-retries

This command configures the number of times the SSH server attempts to reauthenticate a user. Use the **no** form to restore the default setting.

### SYNTAX

**ip ssh authentication-retries** *count*

**no ip ssh authentication-retries**

*count* – The number of authentication attempts permitted after which the interface is reset. (Range: 1-5)

### DEFAULT SETTING

3

### COMMAND MODE

Global Configuration

### EXAMPLE

```
Console(config)#ip ssh authentication-retires 2
Console(config)#
```

### RELATED COMMANDS

show ip ssh (723)

## ip ssh server

This command enables the Secure Shell (SSH) server on this switch. Use the **no** form to disable this service.

### SYNTAX

[**no**] **ip ssh server**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.
- The SSH server uses DSA or RSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.

■You must generate DSA and RSA host keys before enabling the SSH server.

#### EXAMPLE

```
Console#ip ssh crypto host-key generate dsa
Console#configure
Console(config)#ip ssh server
Console(config)#
```

#### RELATED COMMANDS

ip ssh crypto host-key generate (721)
show ssh (725)

### ip ssh server-key size

This command sets the SSH server key size. Use the **no** form to restore the default setting.

#### SYNTAX

**ip ssh server-key size** *key-size*

**no ip ssh server-key size**

*key-size* – The size of server key. (Range: 512-896 bits)

#### DEFAULT SETTING

768 bits

#### COMMAND MODE

Global Configuration

#### COMMAND USAGE

The server key is a private key that is never shared outside the switch.
The host key is shared with the SSH client, and is fixed at 1024 bits.

#### EXAMPLE

```
Console(config)#ip ssh server-key size 512
Console(config)#
```

### ip ssh timeout

This command configures the timeout for the SSH server. Use the **no** form to restore the default setting.

#### SYNTAX

**ip ssh timeout** *seconds*

**no ip ssh timeout**

*seconds* – The timeout for client response during SSH negotiation. (Range: 1-120)

#### DEFAULT SETTING
10 seconds

#### COMMAND MODE
Global Configuration

#### COMMAND USAGE
The **timeout** specifies the interval the switch will wait for a response from the client during the SSH negotiation phase. Once an SSH session has been established, the timeout for user input is controlled by the exec-timeout command for vty sessions.

#### EXAMPLE

```
Console(config)#ip ssh timeout 60
Console(config)#
```

#### RELATED COMMANDS
exec-timeout (632)
show ip ssh (723)

## delete public-key

This command deletes the specified user's public key.

#### SYNTAX

**delete public-key** *username* [**dsa** | **rsa**]

username – Name of an SSH user. (Range: 1-8 characters)

**dsa** – DSA public key type.

**rsa** – RSA public key type.

#### DEFAULT SETTING
Deletes both the DSA and RSA key.

#### COMMAND MODE
Privileged Exec

#### EXAMPLE

```
Console#delete public-key admin dsa
Console#
```

## ip ssh crypto host-key generate

This command generates the host key pair (i.e., public and private).

#### SYNTAX

**ip ssh crypto host-key generate** [**dsa** | **rsa**]

**dsa** – DSA (Version 2) key type.

**rsa** – RSA (Version 1) key type.

### DEFAULT SETTING
Generates both the DSA and RSA key pairs.

### COMMAND MODE
Privileged Exec

### COMMAND USAGE
- The switch uses only RSA Version 1 for SSHv1.5 clients and DSA Version 2 for SSHv2 clients.
- This command stores the host key pair in memory (i.e., RAM). Use the ip ssh save host-key command to save the host key pair to flash memory.
- Some SSH client programs automatically add the public key to the known hosts file as part of the configuration process. Otherwise, you must manually create a known hosts file and place the host public key in it.
- The SSH server uses this host key to negotiate a session key and encryption method with the client trying to connect to it.

### EXAMPLE

```
Console#ip ssh crypto host-key generate dsa
Console#
```

### RELATED COMMANDS
ip ssh crypto zeroize (722)
ip ssh save host-key (723)

## ip ssh crypto zeroize

This command clears the host key from memory (i.e. RAM).

### SYNTAX

**ip ssh crypto zeroize** [**dsa** | **rsa**]

**dsa** – DSA key type.

**rsa** – RSA key type.

### DEFAULT SETTING
Clears both the DSA and RSA key.

### COMMAND MODE
Privileged Exec

### COMMAND USAGE
- This command clears the host key from volatile memory (RAM). Use the **no** ip ssh save host-key command to clear the host key from flash memory.
- The SSH server must be disabled before you can execute this command.

### EXAMPLE

```
Console#ip ssh crypto zeroize dsa
Console#
```

### RELATED COMMANDS

ip ssh crypto host-key generate (721)
ip ssh save host-key (723)
no ip ssh server (719)

## ip ssh save host-key

This command saves the host key from RAM to flash memory.

### SYNTAX

**ip ssh save host-key**

### DEFAULT SETTING

Saves both the DSA and RSA key.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#ip ssh save host-key dsa
Console#
```

### RELATED COMMANDS

ip ssh crypto host-key generate (721)

## show ip ssh

This command displays the connection settings used when authenticating client access to the SSH server.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show ip ssh
SSH Enabled - Version 2.0
Negotiation Timeout : 120 seconds; Authentication Retries : 3
Server Key Size     : 768 bits
Console#
```

## show public-key

This command shows the public key for the specified user or for the host.

### SYNTAX

**show public-key** [**user** [*username*]| **host**]

*username* – Name of an SSH user. (Range: 1-8 characters)

### DEFAULT SETTING

Shows all public keys.

### COMMAND MODE

Privileged Exec

### COMMAND USAGE

- If no parameters are entered, all keys are displayed. If the user keyword is entered, but no user name is specified, then the public keys for all users are displayed.
- When an RSA key is displayed, the first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 35), and the last string is the encoded modulus. When a DSA key is displayed, the first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS), and the last string is the encoded modulus.

### EXAMPLE

```
Console#show public-key host
Host:
RSA:
1024 65537 13236940658254764031382795526536375927835525327972629521130241
  071942106165575942459093923609695405036277525755625100386613098939383452310332 80
  21498886619215955685988798919195058839401813874404689087791603058377681854900028
  31341625008348718449522087429212255691665655296328163516964040831554766066415165
  7116381
DSA:
ssh-dss AAAB3NzaC1kc3MAAACBAPWKZTPbsRIB8ydEXcxM3dyV/yrDbKStIlnzD/Dg0h2Hxc
  YV44sXZ2JXhamLK6P8bvuiyacWbUW/a4PAtp1KMSdqsKeh3hKoA3vRRSy1N2XFfAKxl5fwFfv
  JlPdOkFgzLGMinvSNYQwiQXbKTBH0Z4mUZpE85PWxDZMaCNBPjBrRAAAAFQChb4vsdfQGNIjwb
  vwrNLaQ77isiwAAAIEAsy5YWDC99ebYHNRj5kh47wY4i8cZvH+/p9cnrfwFTMU01VFDly3IR
  2G395NLy5Qd7ZDxfA9mCOfT/yyEfbobMJZi8oGCstSNOxrZZVnMqWrTYfdrKX7YKBw/Kjw6Bm
  iFq7O+jAhf1Dg45loAc27s6TLdtny1wRq/ow2eTCD5nekAAACBAJ8rMccXTxHLFAczWS7EjOy
  DbsloBfPuSAb4oAsyjKXKVYNLQkTLZfcFRu41bS2KV5LAwecsigF/+DjKGWtPNIQqabKgYCw2 o/
  dVzX4Gg+yqdTlYmGA7fHGm8ARGeiG4ssFKy4Z6DmYPXFum1Yg0fhLwuHpOSKdxT3kk475S7
  w0W

Console#
```

**show ssh** This command displays the current SSH server connections.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show ssh
Connection Version State           Username Encryption
  0        2.0   Session-Started     admin    ctos aes128-cbc-hmac-md5
                                     stoc aes128-cbc-hmac-md5
Console#
```

**Table 12: show ssh** - display description

| Field | Description |
|---|---|
| Session | The session number. (Range: 0-3) |
| Version | The Secure Shell version number. |
| State | The authentication negotiation state.<br>(Values: Negotiation-Started, Authentication-Started, Session-Started) |
| Username | The user name of the client. |

## 802.1X PORT AUTHENTICATION

The switch supports IEEE 802.1X (dot1x) port-based access control that prevents unauthorized access to the network by requiring users to first submit credentials for authentication. Client authentication is controlled centrally by a RADIUS server using EAP (Extensible Authentication Protocol).

**Table 13: 802.1X Port Authentication Commands**

| Command | Function | Mode |
|---|---|---|
| *General Commands* | | |
| dot1x default | Resets all dot1x parameters to their default values | GC |
| dot1x eapol-pass-through | Passes EAPOL frames to all ports in STP forwarding state when dot1x is globally disabled | GC |
| dot1x system-auth-control | Enables dot1x globally on the switch. | GC |
| *Authenticator Commands* | | |
| dot1x intrusion-action | Sets the port response to intrusion when authentication fails | IC |
| dot1x max-req | Sets the maximum number of times that the switch retransmits an EAP request/identity packet to the client before it times out the authentication session | IC |
| dot1x operation-mode | Allows single or multiple hosts on an dot1x port | IC |
| dot1x port-control | Sets dot1x mode for a port interface | IC |
| dot1x re-authentication | Enables re-authentication for all ports | IC |

**Table 13: 802.1X Port Authentication Commands (Continued)**

| Command | Function | Mode |
|---|---|---|
| dot1x timeout quiet-period | Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client | IC |
| dot1x timeout re-authperiod | Sets the time period after which a connected client must be re-authenticated | IC |
| dot1x timeout supp-timeout | Sets the interval for a supplicant to respond | IC |
| dot1x timeout tx-period | Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet | IC |
| dot1x re-authenticate | Forces re-authentication on specific ports | PE |
| *Display Information Commands* | | |
| show dot1x | Shows all dot1x related information | PE |

## dot1x default

This command sets all configurable dot1x global and port settings to their default values.

### COMMAND MODE

Global Configuration

### EXAMPLE

```
Console(config)#dot1x default
Console(config)#
```

## dot1x eapol-pass-through

This command passes EAPOL frames through to all ports in STP forwarding state when dot1x is globally disabled. Use the **no** form to restore the default.

### SYNTAX

[**no**] **dot1x eapol-pass-through**

### DEFAULT SETTING

Discards all EAPOL frames when dot1x is globally disabled

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- When this device is functioning as intermediate node in the network and does not need to perform dot1x authentication, the **dot1x eapol pass-through** command can be used to forward EAPOL frames from other switches on to the authentication servers, thereby allowing the authentication process to still be carried out by switches located on the edge of the network.

- When this device is functioning as an edge switch but does not require any attached clients to be authenticated, the **no dot1x eapol-pass-through** command can be used to discard unnecessary EAPOL traffic.

#### EXAMPLE

This example instructs the switch to pass all EAPOL frame through to any ports in STP forwarding state.

```
Console(config)#dot1x eapol-pass-through
Console(config)#
```

## dot1x system-auth-control

This command enables IEEE 802.1X port authentication globally on the switch. Use the **no** form to restore the default.

#### SYNTAX

[**no**] **dot1x system-auth-control**

#### DEFAULT SETTING

Disabled

#### COMMAND MODE

Global Configuration

#### EXAMPLE

```
Console(config)#dot1x system-auth-control
Console(config)#
```

## dot1x intrusion-action

This command sets the port's response to a failed authentication, either to block all traffic, or to assign all traffic for the port to a guest VLAN. Use the **no** form to reset the default.

#### SYNTAX

**dot1x intrusion-action** {**block-traffic** | **guest-vlan**}

**no dot1x intrusion-action**

**block-traffic** - Blocks traffic on this port.

**guest-vlan** - Assigns the user to the Guest VLAN.

#### DEFAULT

block-traffic

#### COMMAND MODE

Interface Configuration

#### COMMAND USAGE

For guest VLAN assignment to be successful, the VLAN must be configured and set as active (see the vlan database command) and assigned as the guest VLAN for the port (see the network-access guest-vlan command).

#### EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x intrusion-action guest-vlan
Console(config-if)#
```

## dot1x max-req

This command sets the maximum number of times the switch port will retransmit an EAP request/identity packet to the client before it times out the authentication session. Use the **no** form to restore the default.

#### SYNTAX

**dot1x max-req** *count*

**no dot1x max-req**

*count* – The maximum number of requests (Range: 1-10)

#### DEFAULT

2

#### COMMAND MODE

Interface Configuration

#### EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-req 2
Console(config-if)#
```

## dot1x operation-mode

This command allows hosts (clients) to connect to an 802.1X-authorized port. Use the **no** form with no keywords to restore the default to single host. Use the **no** form with the **multi-host max-count** keywords to restore the default maximum count.

#### SYNTAX

**dot1x operation-mode** {**single-host** | **multi-host** [**max-count** *count*] | **mac-based-auth**}

**no dot1x operation-mode** [**multi-host max-count**]

**single-host** – Allows only a single host to connect to this port.

**multi-host** – Allows multiple host to connect to this port.

**max-count** – Keyword for the maximum number of hosts.

*count* – The maximum number of hosts that can connect to a port. (Range: 1-1024; Default: 5)

**mac-based** – Allows multiple hosts to connect to this port, with each host needing to be authenticated.

#### DEFAULT

Single-host

#### COMMAND MODE

Interface Configuration

#### COMMAND USAGE

- The "max-count" parameter specified by this command is only effective if the dot1x mode is set to "auto" by the dot1x port-control command.

- In "multi-host" mode, only one host connected to a port needs to pass authentication for all other hosts to be granted network access. Similarly, a port can become unauthorized for all hosts if one attached host fails re-authentication or sends an EAPOL logoff message.

- In "mac-based-auth" mode, each host connected to a port needs to pass authentication. The number of hosts allowed access to a port operating in this mode is limited only by the available space in the secure address table (i.e., up to 1024 addresses).

#### EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x operation-mode multi-host max-count 10
Console(config-if)#
```

### dot1x port-control

This command sets the dot1x mode on a port interface. Use the **no** form to restore the default.

#### SYNTAX

**dot1x port-control** {**auto** | **force-authorized** | **force-unauthorized**}

**no dot1x port-control**

**auto** – Requires a dot1x-aware connected client to be authorized by the RADIUS server. Clients that are not dot1x-aware will be denied access.

**force-authorized** – Configures the port to grant access to all clients, either dot1x-aware or otherwise.

**force-unauthorized** – Configures the port to deny access to all clients, either dot1x-aware or otherwise.

#### DEFAULT

force-authorized

#### COMMAND MODE

Interface Configuration

#### EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x port-control auto
Console(config-if)#
```

## dot1x re-authentication

This command enables periodic re-authentication for a specified port. Use the **no** form to disable re-authentication.

### SYNTAX

[**no**] **dot1x re-authentication**

### COMMAND MODE

Interface Configuration

### COMMAND USAGE

- The re-authentication process verifies the connected client's user ID and password on the RADIUS server. During re-authentication, the client remains connected the network and the process is handled transparently by the dot1x client software. Only if re-authentication fails is the port blocked.

- The connected client is re-authenticated after the interval specified by the dot1x timeout re-authperiod command. The default is 3600 seconds.

### EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x re-authentication
Console(config-if)#
```

### RELATED COMMANDS

dot1x timeout re-authperiod (731)

## dot1x timeout quiet-period

This command sets the time that a switch port waits after the maximum request count (see page 728) has been exceeded before attempting to acquire a new client. Use the **no** form to reset the default.

### SYNTAX

**dot1x timeout quiet-period** *seconds*

**no dot1x timeout quiet-period**

*seconds* - The number of seconds. (Range: 1-65535)

### DEFAULT

60 seconds

### COMMAND MODE

Interface Configuration

### EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout quiet-period 350
Console(config-if)#
```

## dot1x timeout re-authperiod

This command sets the time period after which a connected client must be re-authenticated. Use the **no** form of this command to reset the default.

### SYNTAX

**dot1x timeout re-authperiod** *seconds*

**no dot1x timeout re-authperiod**

*seconds* - The number of seconds. (Range: 1-65535)

### DEFAULT

3600 seconds

### COMMAND MODE

Interface Configuration

### EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout re-authperiod 300
Console(config-if)#
```

## dot1x timeout supp-timeout

This command sets the time that an interface on the switch waits for a response to an EAP request from a client before re-transmitting an EAP packet. Use the **no** form to reset to the default value.

### SYNTAX

**dot1x timeout supp-timeout** *seconds*

**no dot1x timeout supp-timeout**

*seconds* - The number of seconds. (Range: 1-65535)

### DEFAULT

30 seconds

### COMMAND MODE

Interface Configuration

### COMMAND USAGE

This command sets the timeout for EAP-request frames other than EAP-request/identity frames. If dot1x authentication is enabled on a port, the switch will initiate authentication when the port link state comes up. It will send an EAP-request/identity frame to the client to request its identity, followed by one or more requests for authentication information. It may also send other EAP-request frames to the client during an active connection as required for reauthentication.

#### EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout supp-timeout 300
Console(config-if)#
```

## dot1x timeout tx-period

This command sets the time that an interface on the switch waits during an authentication session before re-transmitting an EAP packet. Use the **no** form to reset to the default value.

#### SYNTAX

**dot1x timeout tx-period** *seconds*

**no dot1x timeout tx-period**

*seconds* - The number of seconds. (Range: 1-65535)

#### DEFAULT

30 seconds

#### COMMAND MODE

Interface Configuration

#### EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout tx-period 300
Console(config-if)#
```

## dot1x re-authenticate

This command forces re-authentication on all ports or a specific interface.

#### SYNTAX

**dot1x re-authenticate** [*interface*]

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-26)

#### COMMAND MODE

Privileged Exec

#### COMMAND USAGE

The re-authentication process verifies the connected client's user ID and password on the RADIUS server. During re-authentication, the client remains connected the network and the process is handled transparently by the dot1x client software. Only if re-authentication fails is the port blocked.

### EXAMPLE

```
Console#dot1x re-authenticate
Console#
```

## 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*

*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 (page 727).

- *Authenticator Parameters* – Shows whether or not EAPOL pass-through is enabled (page 726).

- *802.1X Port Summary* – Displays the port access control parameters for each interface that has enabled 802.1X, including the following items:

  - Type – Administrative state for port access control (Enabled, Authenticator, or Supplicant).
  - Operation Mode–Allows single or multiple hosts (page 728).
  - Control Mode– Dot1x port control mode (page 729).
  - Authorized– Authorization status (yes or n/a - not authorized).

- *802.1X Port Details* – Displays the port access control parameters for each interface, including the following items:

  - Reauthentication – Periodic re-authentication (page 730).
  - Reauth Period – Time after which a connected client must be re-authenticated (page 731).
  - Quiet Period – Time a port waits after Max Request Count is exceeded before attempting to acquire a new client (page 730).
  - TX Period – Time a port waits during authentication session before re-transmitting EAP packet (page 732).
  - Supplicant Timeout – Supplicant timeout.
  - Server Timeout – Server timeout.
  - Reauth Max Retries – Maximum number of reauthentication attempts.

- Max Request – Maximum number of times a port will retransmit an EAP request/identity packet to the client before it times out the authentication session (page 728).
- Operation Mode– Shows if single or multiple hosts (clients) can connect to an 802.1X-authorized port.
- Port Control–Shows the dot1x mode on a port as auto, force-authorized, or force-unauthorized (page 729).
- Intrusion Action– Sets the port response to intrusion when authentication fails (page 727).
- Supplicant– MAC address of authorized client.

■ *Authenticator PAE State Machine*

- State – Current state (including initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized).
- Reauth Count– Number of times connecting state is re-entered.
- Current Identifier– The integer (0-255) used by the Authenticator to identify the current authentication session.

■ *Backend State Machine*

- State – Current state (including request, response, success, fail, timeout, idle, initialize).
- Request Count– Number of EAP Request packets sent to the Supplicant without receiving a response.
- Identifier (Server)– Identifier carried in the most recent EAP Success, Failure or Request packet received from the Authentication Server.

■ *Reauthentication State Machine*

State – Current state (including initialize, reauthenticate).

## EXAMPLE

```
Console#show dot1x
Global 802.1X Parameters
 System Auth Control       : Enabled

Authenticator Parameters:
 EAPOL Pass Through        : Disabled

802.1X Port Summary

Port    Type        Operation Mode Control Mode       Authorized
-------- ------------- -------------- ----------------- ----------
1/1       Disabled     Single-Host    ForceAuthorized     N/A
1/2       Disabled     Single-Host    ForceAuthorized     N/A
.
.
1/25      Disabled     Single-Host    ForceAuthorized     Yes
1/26      Enabled      Single-Host    Auto                Yes

802.1X Port Details

802.1X Authenticator is enabled on port 1/1
.
.
.
```

```
802.1X Authenticator is enabled on port 26
Reauthentication     : Enabled
Reauth Period        : 3600
Quiet Period         : 60
TX Period            : 30
Supplicant Timeout   : 30
Server Timeout       : 10
Reauth Max Retries   : 2
Max Request          : 2
Operation Mode       : Multi-host
Port Control         : Auto
Intrusion Action     : Block traffic

Supplicant           : 00-e0-29-94-34-65


 Authenticator PAE State Machine
  State              : Initialize
  Reauth Count       : 0
  Current Identifier : 0

 Authenticator PAE State Machine
  State              : Authenticated
  Reauth Count       : 0
  Current Identifier : 3

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

 Reauthentication State Machine
  State              : Initialize

Console#
```

## MANAGEMENT IP FILTER

This section describes commands used to configure IP management access to the switch.

**Table 14: Management IP Filter Commands**

| Command | Function | Mode |
|---|---|---|
| management | Configures IP addresses that are allowed management access | GC |
| show management | Displays the switch to be monitored or configured from a browser | PE |

## management

This command specifies the client IP addresses that are allowed management access to the switch through various protocols. Use the **no** form to restore the default setting.

### SYNTAX

[**no**] **management** {**all-client** | **http-client** | **snmp-client** | **telnet-client**} *start-address* [*end-address*]

**all-client** - Adds IP address(es) to all groups.

**http-client** - Adds IP address(es) to the web group.

**snmp-client** - Adds IP address(es) to the SNMP group.

**telnet-client** - Adds IP address(es) to the Telnet group.

*start-address* - A single IP address, or the starting address of a range.

*end-address* - The end address of a range.

### DEFAULT SETTING

All addresses

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.

- IP address can be configured for SNMP, web, and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.

- When entering addresses for the same group (i.e., SNMP, web, or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.

- You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.

- You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

### EXAMPLE

This example restricts management access to the indicated addresses.

```
Console(config)#management all-client 192.168.1.19
Console(config)#management all-client 192.168.1.25 192.168.1.30
Console#
```

## show management

This command displays the client IP addresses that are allowed management access to the switch through various protocols.

### SYNTAX

**show management** {**all-client** | **http-client** | **snmp-client** | **telnet-client**}

**all-client** - Displays IP addresses for all groups.

**http-client** - Displays IP addresses for the web group.

**snmp-client** - Displays IP addresses for the SNMP group.

**telnet-client** - Displays IP addresses for the Telnet group.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show management all-client
Management IP Filter
 HTTP Client:
Start IP Address                End IP Address
-------------------------------------- ----------------------------------
192.168.1.19                    192.168.1.19

 SNMP Client:
Start IP Address                End IP Address
-------------------------------------- -------------------------------------
192.168.1.19                    192.168.1.19

 Telnet Client:
Start IP Address                End IP Address
-------------------------------------- -------------------------------------
192.168.1.19                    192.168.1.19

Console#
```

# 30 GENERAL SECURITY MEASURES

This switch supports many methods of segregating traffic for clients attached to each of the data ports, and for ensuring that only authorized clients gain access to the network. Private VLANs and Port-based authentication using IEEE 802.1X are commonly used for these purposes. In addition to these method, several other options of providing client security are described in this chapter. These include port-based authentication, which can be configured to allow network client access by specifying a fixed set of MAC addresses. The addresses assigned to DHCP clients can also be carefully controlled with IP Source Guard and DHCP Snooping commands.

**Table 1: General Security Commands**

| Command Group | Function |
|---|---|
| Port Security[1] | Configures secure addresses for a port |
| 802.1X Port Authentication* | Configures host authentication on specific ports using 802.1X |
| Network Access* | Configures MAC authentication and dynamic VLAN assignment |
| Web Authentication* | Configures Web authentication |
| Access Control Lists* | Provides filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or non-IP frames (based on MAC address or Ethernet type) |
| DHCP Snooping* | Filters untrusted DHCP messages on unsecure ports by building and maintaining a DHCP snooping binding table |
| IP Source Guard* | Filters IP traffic on insecure ports for which the source address cannot be identified via DHCP snooping nor static source bindings |
| ARP Inspection | Validates the MAC-to-IP address bindings in ARP packets |

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

# Port Security

These commands can be used to enable port security on a port.

When MAC address learning is disabled on an interface, only incoming traffic with source addresses already stored in the dynamic or static address table for this port will be authorized to access the network.

When using port security, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table for this port will be authorized to access the network. The port will drop any incoming frames with a source MAC address that is unknown or has been previously learned from another port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

**Table 2: Management IP Filter Commands**

| Command | Function | Mode |
|---|---|---|
| mac-address-table static | Maps a static address to a port in a VLAN | GC |
| mac-learning | Enables MAC address learning on the selected physical interface or VLAN | IC |
| port security | Configures a secure port | IC |
| show mac-address-table | Displays entries in the bridge-forwarding database | PE |

## mac-learning

This command enables MAC address learning on the selected interface. Use the **no** form to disable MAC address learning.

### Syntax

[**no**] **mac-learning**

### Default Setting

Enabled

### Command Mode

Interface Configuration (Ethernet or Port Channel)

### Command Usage

- The **no mac-learning** command immediately stops the switch from learning new MAC addresses on the specified port or trunk. Only incoming traffic with source addresses stored in the static address table will be accepted. Note that the dynamic addresses stored in the address table when MAC address learning is disabled are flushed from the system, and no dynamic addresses are subsequently learned until MAC address learning has been re-enabled.

- The mac-learning commands cannot be used if 802.1X Port Authentication has been globally enabled on the switch with the dot1x system-auth-control command, or if MAC Address Security has been enabled by the port security command on the same interface.

### EXAMPLE

The following example disables MAC address learning for port 2.

```
Console(config)#interface ethernet 1/2
Console(config-if)#no mac-learning
Console(config-if)#
```

### RELATED COMMANDS

show interfaces status (816)

## port security

This command enables or configures port security. Use the **no** form without any keywords to disable port security. Use the **no** form with the appropriate keyword to restore the default settings for a response to security violation or for the maximum number of allowed addresses.

### SYNTAX

**port security** [**action** {**shutdown** | **trap** | **trap-and-shutdown**} | **max-mac-count** *address-count*]

**no port security** [**action** | **max-mac-count**]

**action** - Response to take when port security is violated.

**shutdown** - Disable port only.

**trap** - Issue SNMP trap message only.

**trap-and-shutdown** - Issue SNMP trap message and disable port.

**max-mac-count**

*address-count* - The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 1024, where 0 means disabled)

### DEFAULT SETTING

Status: Disabled
Action: None
Maximum Addresses: 0

### COMMAND MODE

Interface Configuration (Ethernet)

### COMMAND USAGE

■ When port security is enabled with this command, the switch first clears all dynamically learned entries from the address table. It then starts learning new MAC addresses on the specified port, and stops learning addresses when it reaches a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted.

- First use the **port security max-mac-count** command to set the number of addresses, and then use the **port security** command to enable security on the port. (The specified maximum address count is effective when port security is enabled or disabled.)

- Use the **no port security max-mac-count** command to disable port security and reset the maximum number of addresses to the default.

- You can also manually add secure addresses with the mac-address-table static command.

- A secure port has the following restrictions:

  - Cannot be connected to a network interconnection device.
  - Cannot be a trunk port.

- If a port is disabled due to a security violation, it must be manually re-enabled using the no shutdown command.

### EXAMPLE

The following example enables port security for port 5, and sets the response to a security violation to issue a trap message:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap
```

### RELATED COMMANDS

show interfaces status (816)
shutdown (811)
mac-address-table static (854)

## NETWORK ACCESS (MAC ADDRESS AUTHENTICATION)

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

**Table 3: Network Access Commands**

| Command | Function | Mode |
|---|---|---|
| network-access aging | Enables MAC address aging | GC |
| network-access mac-filter | Adds a MAC address to a filter table | GC |
| mac-authentication reauth-time | Sets the time period after which a connected MAC address must be re-authenticated | GC |
| network-access dynamic-qos | Enables the dynamic quality of service feature | IC |

**Table 3: Network Access Commands**

| Command | Function | Mode |
|---|---|---|
| network-access dynamic-vlan | Enables dynamic VLAN assignment from a RADIUS server | IC |
| network-access guest-vlan | Specifies the guest VLAN | IC |
| network-access link-detection | Enables the link detection feature | IC |
| network-access link-detection link-down | Configures the link detection feature to detect and act upon link-down events | IC |
| network-access link-detection link-up | Configures the link detection feature to detect and act upon link-up events | IC |
| network-access link-detection link-up-down | Configures the link detection feature to detect and act upon both link-up and link-down events | IC |
| network-access max-mac-count | Sets the maximum number of MAC addresses that can be authenticated on a port via all forms of authentication | IC |
| network-access mode mac-authentication | Enables MAC authentication on an interface | IC |
| network-access port-mac-filter | Enables the specified MAC address filter | IC |
| mac-authentication intrusion-action | Determines the port response when a connected host fails MAC authentication. | IC |
| mac-authentication max-mac-count | Sets the maximum number of MAC addresses that can be authenticated on a port via MAC authentication | IC |
| show network-access | Displays the MAC authentication settings for port interfaces | PE |
| show network-access mac-address-table | Displays information for entries in the secure MAC address table | PE |
| show network-access mac-filter | Displays information for entries in the MAC filter tables | PE |

## network-access aging

Use this command to enable aging for authenticated MAC addresses stored in the secure MAC address table. Use the **no** form of this command to disable address aging.

### SYNTAX

[**no**] **network-access aging**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- Authenticated MAC addresses are stored as dynamic entries in the switch's secure MAC address table and are removed when the aging time expires. The address aging time is determined by the mac-address-table aging-time command.

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

Mode (Single-Host, Multi-Host, or MAC-Based authentication as described on page 728).

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

### Example

```
Console(config-if)#network-access aging
Console(config-if)#
```

## network-access mac-filter

Use this command to add a MAC address into a filter table. Use the **no** form of this command to remove the specified MAC address.

### Syntax

[**no**] **network-access mac-filter** *filter-id*
**mac-address** *mac-address* [**mask** *mask-address*]

*filter-id* - Specifies a MAC address filter table. (Range: 1-64)

*mac-address* - Specifies a MAC address entry.
(Format: xx-xx-xx-xx-xx-xx)

*mask* - Specifies a MAC address bit mask for a range of addresses.

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

- Specified addresses are exempt from network access authentication.

- This command is different from configuring static addresses with the mac-address-table static command in that it allows you configure a range of addresses when using a mask, and then to assign these addresses to one or more ports with the network-access port-mac-filter command.

- Up to 64 filter tables can be defined.

- There is no limitation on the number of entries that can entered in a filter table.

### Example

```
Console(config)#network-access mac-filter 1 mac-address 11-22-33-44-55-66
Console(config)#
```

## mac-authentication reauth-time

Use this command to set the time period after which a connected MAC address must be re-authenticated. Use the **no** form of this command to restore the default value.

### SYNTAX

**mac-authentication reauth-time** *seconds*

**no mac-authentication reauth-time**

*seconds* - The reauthentication time period.
(Range: 120-1000000 seconds)

### DEFAULT SETTING

1800

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- The reauthentication time is a global setting and applies to all ports.
- When the reauthentication time expires for a secure MAC address it is reauthenticated with the RADIUS server. During the reauthentication process traffic through the port remains unaffected.

### EXAMPLE

```
Console(config)#mac-authentication reauth-time 300
Console(config)#
```

## network-access dynamic-qos

Use this command to enable the dynamic QoS feature for an authenticated port. Use the **no** form to restore the default.

### SYNTAX

[**no**] **network-access dynamic-qos**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Interface Configuration

### Command Usage

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

**Table 4: Dynamic QoS Profiles**

| Profile | Attribute Syntax | Example |
|---|---|---|
| DiffServ | **service-policy-in**=*policy-map-name* | service-policy-in=p1 |
| Rate Limit | **rate-limit-input**=*rate* | rate-limit-input=100 (Kbps) |
| 802.1p | **switchport-priority-default**=*value* | switchport-priority-default=2 |
| IP ACL | **ip-access-group-in**=*ip-acl-name* | ip-access-group-in=ipv4acl |
| IPv6 ACL | **ipv6-access-group-in**=*ipv6-acl-name* | ipv6-access-group-in=ipv6acl |
| MAC ACL | **mac-access-group-in**=*mac-acl-name* | mac-access-group-in=macAcl |

- When the last user logs off of a port with a dynamic QoS assignment, the switch restores the original QoS configuration for the port.

- When a user attempts to log into the network with a returned dynamic QoS profile that is different from users already logged on to the same port, the user is denied access.

- While a port has an assigned dynamic QoS profile, any manual QoS configuration changes only take effect after all users have logged off of the port.

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

### Example

The following example enables the dynamic QoS feature on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access dynamic-qos
Console(config-if)#
```

## network-access dynamic-vlan

Use this command to enable dynamic VLAN assignment for an authenticated port. Use the **no** form to disable dynamic VLAN assignment.

### Syntax

[**no**] **network-access dynamic-vlan**

### Default Setting

Enabled

### Command Mode

Interface Configuration

#### COMMAND USAGE

- When enabled, the VLAN identifiers returned by the RADIUS server will be applied to the port, providing the VLANs have already been created on the switch. GVRP is not used to create the VLANs.
- The VLAN settings specified by the first authenticated MAC address are implemented for a port. Other authenticated MAC addresses on the port must have same VLAN configuration, or they are treated as an authentication failure.
- If dynamic VLAN assignment is enabled on a port and the RADIUS server returns no VLAN configuration, the authentication is still treated as a success, and the host assigned to the default untagged VLAN.
- When the dynamic VLAN assignment status is changed on a port, all authenticated addresses are cleared from the secure MAC address table.

#### EXAMPLE

The following example enables dynamic VLAN assignment on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access dynamic-vlan
Console(config-if)#
```

### network-access guest-vlan

Use this command to assign all traffic on a port to a guest VLAN when 802.1x authentication is rejected. Use the **no** form of this command to disable guest VLAN assignment.

#### SYNTAX

**network-access guest-vlan** *vlan-id*

**no network-access guest-vlan**

*vlan-id* - VLAN ID (Range: 1-4093)

#### DEFAULT SETTING

Disabled

#### COMMAND MODE

Interface Configuration

#### COMMAND USAGE

- The VLAN to be used as the guest VLAN must be defined and set as active (See the vlan database command).
- When used with 802.1X authentication, the intrusion-action must be set for “guest-vlan” to be effective (see the dot1x intrusion-action command).

#### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access guest-vlan 25
Console(config-if)#
```

## network-access link-detection

Use this command to enable link detection for the selected port. Use the **no** form of this command to restore the default.

### Syntax

[**no**] **network-access link-detection**

### Default Setting

Disabled

### Command Mode

Interface Configuration

### Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection
Console(config-if)#
```

## network-access link-detection link-down

Use this command to detect link-down events. When detected, the switch can shut down the port, send an SNMP trap, or both. Use the **no** form of this command to disable this feature.

### Syntax

**network-access link-detection link-down**
**action** [**shutdown** | **trap** | **trap-and-shutdown**]

**no network-access link-detection**

- **action** - Response to take when port security is violated.
  - **shutdown** - Disable port only.
  - **trap** - Issue SNMP trap message only.
  - **trap-and-shutdown** - Issue SNMP trap message and disable the port.

### Default Setting

Disabled

### Command Mode

Interface Configuration

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection link-down action trap
Console(config-if)#
```

## network-access link-detection link-up

Use this command to detect link-up events. When detected, the switch can shut down the port, send an SNMP trap, or both. Use the **no** form of this command to disable this feature.

### SYNTAX

**network-access link-detection link-up**
**action** [**shutdown** | **trap** | **trap-and-shutdown**]

**no network-access link-detection**

**action** - Response to take when port security is violated.

**shutdown** - Disable port only.

**trap** - Issue SNMP trap message only.

**trap-and-shutdown** - Issue SNMP trap message and disable the port.

### DEFAULT SETTING

Disabled

### COMMAND MODE

Interface Configuration

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection link-up action trap
Console(config-if)#
```

## network-access link-detection link-up-down

Use this command to detect link-up and link-down events. When either event is detected, the switch can shut down the port, send an SNMP trap, or both. Use the **no** form of this command to disable this feature.

### SYNTAX

**network-access link-detection link-up-down**
**action** [**shutdown** | **trap** | **trap-and-shutdown**]

**no network-access link-detection**

**action** - Response to take when port security is violated.

**shutdown** - Disable port only.

**trap** - Issue SNMP trap message only.

**trap-and-shutdown** - Issue SNMP trap message and disable the port.

**Default Setting**
Disabled

**Command Mode**
Interface Configuration

**Example**

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection link-up-down action trap
Console(config-if)#
```

## network-access max-mac-count

Use this command to set the maximum number of MAC addresses that can be authenticated on a port interface via all forms of authentication. Use the **no** form of this command to restore the default.

**Syntax**

**network-access max-mac-count** *count*

**no network-access max-mac-count**

*count* - The maximum number of authenticated IEEE 802.1X and MAC addresses allowed. (Range: 0-1024; 0 for unlimited)

**Default Setting**
1024

**Command Mode**
Interface Configuration

**Command Usage**
The maximum number of MAC addresses per port is 1024, and the maximum number of secure MAC addresses supported for the switch system is 1024. When the limit is reached, all new MAC addresses are treated as authentication failures.

**Example**

```
Console(config-if)#network-access max-mac-count 5
Console(config-if)#
```

## network-access mode mac-authentication

Use this command to enable network access authentication on a port. Use the **no** form of this command to disable network access authentication.

**Syntax**

[**no**] **network-access mode mac-authentication**

**Default Setting**
Disabled

### COMMAND MODE
Interface Configuration

### COMMAND USAGE
- When enabled on a port, the authentication process sends a Password Authentication Protocol (PAP) request to a configured RADIUS server. The user name and password are both equal to the MAC address being authenticated.
- On the RADIUS server, PAP user name and passwords must be configured in the MAC address format XX-XX-XX-XX-XX-XX (all in upper case).
- Authenticated MAC addresses are stored as dynamic entries in the switch secure MAC address table and are removed when the aging time expires. The maximum number of secure MAC addresses supported for the switch system is 1024.
- Configured static MAC addresses are added to the secure address table when seen on a switch port. Static addresses are treated as authenticated without sending a request to a RADIUS server.
- MAC authentication, 802.1X, and port security cannot be configured together on the same port. Only one security mechanism can be applied.
- MAC authentication cannot be configured on trunk ports.
- When port status changes to down, all MAC addresses are cleared from the secure MAC address table. Static VLAN assignments are not restored.
- The RADIUS server may optionally return a VLAN identifier list. VLAN identifier list is carried in the “Tunnel-Private-Group-ID” attribute. The VLAN list can contain multiple VLAN identifiers in the format “1u,2t,” where “u” indicates untagged VLAN and “t” tagged VLAN. The “Tunnel-Type” attribute should be set to “VLAN,” and the “Tunnel-Medium-Type” attribute set to “802.”

### EXAMPLE
```
Console(config-if)#network-access mode mac-authentication
Console(config-if)#
```

## network-access port-mac-filter

Use this command to enable the specified MAC address filter. Use the **no** form of this command to disable the specified MAC address filter.

### SYNTAX

**network-access port-mac-filter** *filter-id*

**no network-access port-mac-filter**

*filter-id* - Specifies a MAC address filter table. (Range: 1-64)

### DEFAULT SETTING
None

**COMMAND MODE**

Interface Configuration

**COMMAND MODE**

- Entries in the MAC address filter table can be configured with the network-access mac-filter command.
- Only one filter table can be assigned to a port.

**EXAMPLE**

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access port-mac-filter 1
Console(config-if)#
```

## mac-authentication intrusion-action

Use this command to configure the port response to a host MAC authentication failure. Use the **no** form of this command to restore the default.

**SYNTAX**

**mac-authentication intrusion-action** {**block traffic** | **pass traffic**}

**no mac-authentication intrusion-action**

**DEFAULT SETTING**

Block Traffic

**COMMAND MODE**

Interface Configuration

**EXAMPLE**

```
Console(config-if)#mac-authentication intrusion-action block-traffic
Console(config-if)#
```

## mac-authentication max-mac-count

Use this command to set the maximum number of MAC addresses that can be authenticated on a port via MAC authentication. Use the **no** form of this command to restore the default.

**SYNTAX**

**mac-authentication max-mac-count** *count*

**no mac-authentication max-mac-count**

*count* - The maximum number of MAC-authenticated MAC addresses allowed. (Range: 1-1024)

**DEFAULT SETTING**

1024

### COMMAND MODE
Interface Configuration

### EXAMPLE

```
Console(config-if)#mac-authentication max-mac-count 32
Console(config-if)#
```

## show network-access

Use this command to display the MAC authentication settings for port interfaces.

### SYNTAX

**show network-access** [**interface** *interface*]

*interface* - Specifies a port interface.

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

### DEFAULT SETTING
Displays the settings for all interfaces.

### COMMAND MODE
Privileged Exec

### EXAMPLE

```
Console#show network-access interface ethernet 1/1
Global secure port information
Reauthentication Time                  : 1800
--------------------------------------------------
--------------------------------------------------
Port : 1/1
MAC Authentication                     : Disabled
MAC Authentication Intrusion action    : Block traffic
MAC Authentication Maximum MAC Counts : 1024
Maximum MAC Counts                     : 2048
Dynamic VLAN Assignment                : Enabled
Guest VLAN                             : Disabled
Console#
```

## show network-access mac-address-table

Use this command to display secure MAC address table entries.

### Syntax

**show network-access mac-address-table** [**static** | **dynamic**] [**address** *mac-address* [*mask*]] [**interface** *interface*] [**sort** {**address** | **interface**}]

**static** - Specifies static address entries.

**dynamic** - Specifies dynamic address entries.

*mac-address* - Specifies a MAC address entry.
(Format: xx-xx-xx-xx-xx-xx)

*mask* - Specifies a MAC address bit mask for filtering displayed addresses.

*interface* - Specifies a port interface.

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**sort** - Sorts displayed entries by either MAC address or interface.

### Default Setting

Displays all filters.

### Command Mode

Privileged Exec

### Command Usage

When using a bit mask to filter displayed MAC addresses, a 1 means “care” and a 0 means “don't care”. For example, a MAC of 00-00-01-02-03-04 and mask FF-FF-FF-00-00-00 would result in all MACs in the range 00-00-01-00-00-00 to 00-00-01-FF-FF-FF to be displayed. All other MACs would be filtered out.

### Example

```
Console#show network-access mac-address-table
---- ----------------- --------------- --------- -------------------------
Port MAC-Address       RADIUS-Server   Attribute Time
---- ----------------- --------------- --------- -------------------------
1/1  00-00-01-02-03-04 172.155.120.17  Static    00d06h32m50s
1/1  00-00-01-02-03-05 172.155.120.17  Dynamic   00d06h33m20s
1/1  00-00-01-02-03-06 172.155.120.17  Static    00d06h35m10s
1/3  00-00-01-02-03-07 172.155.120.17  Dynamic   00d06h34m20s

Console#
```

### show network-access mac-filter

Use this command to display information for entries in the MAC filter tables.

**Syntax**

**show network-access mac-filter** [*filter-id*]

*filter-id* - Specifies a MAC address filter table. (Range: 1-64)

**Default Setting**
Displays all filters.

**Command Mode**
Privileged Exec

**Example**

```
Consoleshownetwork-access mac-filter
Filter ID MAC Address       MAC Mask
--------- ----------------- -----------------
        1 00-00-01-02-03-08 FF-FF-FF-FF-FF-FF
Console#
```

## Web Authentication

Web authentication allows stations to authenticate and access the network in situations where 802.1X or Network Access authentication are infeasible or impractical. The web authentication feature allows unauthenticated hosts to request and receive a DHCP assigned IP address and perform DNS queries. All other traffic, except for HTTP protocol traffic, is blocked. The switch intercepts HTTP protocol traffic and redirects it to a switch-generated web page that facilitates user name and password authentication via RADIUS. Once authentication is successful, the web browser is forwarded on to the originally requested web page. Successful authentication is valid for all hosts connected to the port.

**Note:** RADIUS authentication must be activated and configured for the web authentication feature to work properly (see "Authentication Sequence" on page 693).

**Note:** Web authentication cannot be configured on trunk ports.

**Table 5: Web Authentication**

| Command | Function | Mode |
|---|---|---|
| web-auth login-attempts | Defines the limit for failed web authentication login attempts | GC |
| web-auth quiet-period | Defines the amount of time to wait after the limit for failed login attempts is exceeded. | GC |
| web-auth session-timeout | Defines the amount of time a session remains valid | GC |
| web-auth system-auth-control | Enables web authentication globally for the switch | GC |
| web-auth | Enables web authentication for an interface | IC |

**Table 5: Web Authentication (Continued)**

| Command | Function | Mode |
|---|---|---|
| web-auth re-authenticate (Port) | Ends all web authentication sessions on the port and forces the users to re-authenticate | PE |
| web-auth re-authenticate (IP) | Ends the web authentication session associated with the designated IP address and forces the user to re-authenticate | PE |
| show web-auth | Displays global web authentication parameters | PE |
| show web-auth interface | Displays interface-specific web authentication parameters and statistics | PE |
| show web-auth summary | Displays a summary of web authentication port parameters and statistics | PE |

## web-auth login-attempts

This command defines the limit for failed web authentication login attempts. After the limit is reached, the switch refuses further login attempts until the quiet time expires. Use the **no** form to restore the default.

### Syntax

**web-auth login-attempts** *count*

**no web-auth login-attempts**

*count* - The limit of allowed failed login attempts. (Range: 1-3)

### Default Setting

3 login attempts

### Command Mode

Global Configuration

### Example

```
Console(config)#web-auth login-attempts 2
Console(config)#
```

## web-auth quiet-period

This command defines the amount of time a host must wait after exceeding the limit for failed login attempts, before it may attempt web authentication again. Use the **no** form to restore the default.

### Syntax

**web-auth quiet-period** *time*

**no web-auth quiet period**

*time* - The amount of time the host must wait before attempting authentication again. (Range: 1-180 seconds)

### Default Setting

60 seconds

### COMMAND MODE
Global Configuration

### EXAMPLE

```
Console(config)#web-auth quiet-period 120
Console(config)#
```

## web-auth session-timeout

This command defines the amount of time a web-authentication session remains valid. When the session timeout has been reached, the host is logged off and must re-authenticate itself the next time data transmission takes place. Use the **no** form to restore the default.

### SYNTAX

**web-auth session-timeout** *timeout*

**no web-auth session timeout**

*timeout* - The amount of time that an authenticated session remains valid. (Range: 300-3600 seconds)

### DEFAULT SETTING
3600 seconds

### COMMAND MODE
Global Configuration

### EXAMPLE

```
Console(config)#web-auth session-timeout 1800
Console(config)#
```

## web-auth system-auth-control

This command globally enables web authentication for the switch. Use the **no** form to restore the default.

### SYNTAX

[**no**] **web-auth system-auth-control**

### DEFAULT SETTING
Disabled

### COMMAND MODE
Global Configuration

### COMMAND USAGE
Both **web-auth system-auth-control** for the switch and web-auth for an interface must be enabled for the web authentication feature to be active.

#### Example

```
Console(config)#web-auth system-auth-control
Console(config)#
```

## web-auth

This command enables web authentication for an interface. Use the no form to restore the default.

#### Syntax

[**no**] **web-auth**

#### Default Setting

Disabled

#### Command Mode

Interface Configuration

#### Command Usage

Both web-auth system-auth-control for the switch and **web-auth** for a port must be enabled for the web authentication feature to be active.

#### Example

```
Console(config-if)#web-auth
Console(config-if)#
```

## web-auth re-authenticate (Port)

This command ends all web authentication sessions connected to the port and forces the users to re-authenticate.

#### Syntax

**web-auth re-authenticate interface** *interface*

*interface* - Specifies a port interface.

**ethernet** *unit*/*port*

*unit* - This is unit 1.

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

#### Default Setting

None

#### Command Mode

Privileged Exec

### EXAMPLE

```
Console#web-auth re-authenticate interface ethernet 1/2
Failed to reauth.
Console#
```

## web-auth re-authenticate (IP)

This command ends the web authentication session associated with the designated IP address and forces the user to re-authenticate.

### SYNTAX

**web-auth re-authenticate interface** *interface ip*

*interface* - Specifies a port interface.

**ethernet** *unit*/*port*

*unit* - This is unit 1.

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

*ip* - IPv4 formatted IP address

### DEFAULT SETTING

None

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#web-auth re-authenticate interface ethernet 1/2 192.168.1.5
Failed to reauth port.
Console#
```

## show web-auth

This command displays global web authentication parameters.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show web-auth

Global Web-Auth Parameters

  System Auth Control      : Enabled
  Session Timeout          : 3600
  Quiet Period             : 60
  Max Login Attempts       : 3
Console#
```

## show web-auth interface

This command displays interface-specific web authentication parameters and statistics.

### SYNTAX

**show web-auth interface** *interface*

*interface* - Specifies a port interface.

**ethernet** *unit*/*port*

*unit* - This is unit 1.

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show web-auth interface ethernet 1/2
Web Auth Status      : Enabled

Host Summary

IP address      Web-Auth-State Remaining-Session-Time
--------------- -------------- ----------------------
1.1.1.1         Authenticated  295
1.1.1.2         Authenticated  111
Console#
```

## show web-auth summary

This command displays a summary of web authentication port parameters and statistics.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show web-auth summary

Global Web-Auth Parameters

 System Auth Control      : Enabled
Port      Status         Authenticated Host Count
----      ------         ------------------------
1/ 1      Disabled       0
1/ 2      Enabled        8
1/ 3      Disabled       0
1/ 4      Disabled       0
1/ 5      Disabled       0
:
```

## DHCP Snooping

DHCP snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port. This section describes commands used to configure DHCP snooping.

**Table 6: DHCP Snooping Commands**

| Command | Function | Mode |
|---|---|---|
| ip dhcp snooping | Enables DHCP snooping globally | GC |
| ip dhcp snooping database flash | Writes all dynamically learned snooping entries to flash memory | GC |
| ip dhcp snooping information option | Enables or disables DHCP Option 82 information relay | GC |
| ip dhcp snooping information policy | Sets the information option policy for DHCP client packets that include Option 82 information | GC |
| ip dhcp snooping verify mac-address | Verifies the client's hardware address stored in the DHCP packet against the source MAC address in the Ethernet header | GC |
| ip dhcp snooping vlan | Enables DHCP snooping on the specified VLAN | GC |
| ip dhcp snooping trust | Configures the specified interface as trusted | IC |
| clear ip dhcp snooping database flash | Removes all dynamically learned snooping entries from flash memory. | PE |
| show ip dhcp snooping | Shows the DHCP snooping configuration settings | PE |
| show ip dhcp snooping binding | Shows the DHCP snooping binding table entries | PE |

### ip dhcp snooping

This command enables DHCP snooping globally. Use the **no** form to restore the default setting.

#### Syntax

[**no**] **ip dhcp snooping**

#### Default Setting

Disabled

#### Command Mode

Global Configuration

#### Command Usage

- Network traffic may be disrupted when malicious DHCP messages are received from an outside source. DHCP snooping is used to filter DHCP messages received on an unsecure interface from outside the network or fire wall. When DHCP snooping is enabled globally by this command, and enabled on a VLAN interface by the ip dhcp snooping vlan command, DHCP messages received on an untrusted interface (as specified by the no ip dhcp snooping trust command) from a device not listed in the DHCP snooping table will be dropped.

- When enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.

- Table entries are only learned for trusted interfaces. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier.

- When DHCP snooping is enabled, the rate limit for the number of DHCP messages that can be processed by the switch is 100 packets per second. Any DHCP packets in excess of this limit are dropped.

- Filtering rules are implemented as follows:

  - If the global DHCP snooping is disabled, all DHCP packets are forwarded.

  - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a *trusted* port. If the received packet is a DHCP ACK message, a dynamic DHCP snooping entry is also added to the binding table.

  - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is *not trusted*, it is processed as follows:

    - If the DHCP packet is a reply packet from a DHCP server (including OFFER, ACK or NAK messages), the packet is dropped.
    - If the DHCP packet is from a client, such as a DECLINE or RELEASE message, the switch forwards the packet only if the corresponding entry is found in the binding table.
    - If the DHCP packet is from client, such as a DISCOVER, REQUEST, INFORM, DECLINE or RELEASE message, the packet is forwarded if MAC address verification is disabled (as specified by the ip dhcp snooping verify mac-address command). However, if MAC address verification is enabled, then the packet will only be forwarded if the client's hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.
    - If the DHCP packet is not a recognizable type, it is dropped.

  - If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.

  - If a DHCP packet is from server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.

- If the DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.

- *Additional considerations when the switch itself is a DHCP client* – The port(s) through which the switch submits a client request to the DHCP server must be configured as trusted (using the ip dhcp snooping trust command). Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCP server. Also, when the switch sends out DHCP client packets for itself, no filtering takes place. However, when the switch receives any messages from a DHCP server, any packets received from untrusted ports are dropped.

#### EXAMPLE

This example enables DHCP snooping globally for the switch.

```
Console(config)#ip dhcp snooping
Console(config)#
```

#### RELATED COMMANDS

ip dhcp snooping vlan (765)
ip dhcp snooping trust (766)

### ip dhcp snooping database flash

This command writes all dynamically learned snooping entries to flash memory.

#### COMMAND MODE

Privileged Exec

#### COMMAND USAGE

This command can be used to store the currently learned dynamic DHCP snooping entries to flash memory. These entries will be restored to the snooping table when the switch is reset. However, note that the lease time shown for a dynamic entry that has been restored from flash memory will no longer be valid.

#### EXAMPLE

```
Console(config)#ip dhcp snooping database flash
Console(config)#
```

### ip dhcp snooping information option

This command enables the DHCP Option 82 information relay for the switch. Use the **no** form to disable this function.

#### SYNTAX

[**no**] **ip dhcp snooping information option**

#### DEFAULT SETTING

Disabled

#### COMMAND MODE

Global Configuration

#### COMMAND USAGE

- DHCP provides a relay mechanism for sending information about the switch and its DHCP clients to the DHCP server. Known as DHCP Option 82, it allows compatible DHCP servers to use the information when assigning IP addresses, or to set other services or policies for clients.

- When the DHCP Snooping Information Option is enabled, the requesting client (or an intermediate relay agent that has used the information fields to describe itself) can be identified in the DHCP request packets forwarded by the switch and in reply packets sent back from the DHCP server by the switch port to which they are connected rather than just their MAC address. DHCP client-server exchange messages are then forwarded directly between the server and client without having to flood them to the entire VLAN.

- DHCP snooping must be enabled on the switch for the DHCP Option 82 information to be inserted into packets.

- Use the **ip dhcp snooping information option** command to specify how to handle DHCP client request packets which already contain Option 82 information.

### EXAMPLE

This example enables the DHCP Snooping Information Option.

```
Console(config)#ip dhcp snooping information option
Console(config)#
```

## ip dhcp snooping information policy

This command sets the DHCP snooping information option policy for DHCP client packets that include Option 82 information.

### SYNTAX

**ip dhcp snooping information policy** {**drop** | **keep** | **replace**}

**drop** - Drops the client's request packet instead of relaying it.

**keep** - Retains the Option 82 information in the client request, and forwards the packets to trusted ports.

**replace** - Replaces the Option 82 information circuit-id and remote-id fields in the client's request with information about the relay agent itself, inserts the relay agent's address (when DHCP snooping is enabled), and forwards the packets to trusted ports.

### DEFAULT SETTING

replace

### COMMAND MODE

Global Configuration

### COMMAND USAGE

When the switch receives DHCP packets from clients that already include DHCP Option 82 information, the switch can be configured to set the action policy for these packets. The switch can either drop the DHCP packets, keep the existing information, or replace it with the switch's relay information.

#### EXAMPLE

```
Console(config)#ip dhcp snooping information policy drop
Console(config)#
```

### ip dhcp snooping verify mac-address

This command verifies the client's hardware address stored in the DHCP packet against the source MAC address in the Ethernet header. Use the **no** form to disable this function.

#### SYNTAX

[**no**] **ip dhcp binding verify mac-address**

#### DEFAULT SETTING

Enabled

#### COMMAND MODE

Global Configuration

#### COMMAND USAGE

If MAC address verification is enabled, and the source MAC address in the Ethernet header of the packet is not same as the client's hardware address in the DHCP packet, the packet is dropped.

#### EXAMPLE

This example enables MAC address verification.

```
Console(config)#ip dhcp snooping verify mac-address
Console(config)#
```

#### RELATED COMMANDS

ip dhcp snooping (761)
ip dhcp snooping vlan (765)
ip dhcp snooping trust (766)

### ip dhcp snooping vlan

This command enables DHCP snooping on the specified VLAN. Use the **no** form to restore the default setting.

#### SYNTAX

[**no**] **ip dhcp snooping vlan** *vlan-id*

*vlan-id* - ID of a configured VLAN (Range: 1-4093)

#### DEFAULT SETTING

Disabled

#### COMMAND MODE

Global Configuration

**COMMAND USAGE**

- When DHCP snooping enabled globally using the ip dhcp snooping command, and enabled on a VLAN with this command, DHCP packet filtering will be performed on any untrusted ports within the VLAN as specified by the ip dhcp snooping trust command.

- When the DHCP snooping is globally disabled, DHCP snooping can still be configured for specific VLANs, but the changes will not take effect until DHCP snooping is globally re-enabled.

- When DHCP snooping is globally enabled, configuration changes for specific VLANs have the following effects:

  - If DHCP snooping is disabled on a VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.

**EXAMPLE**

This example enables DHCP snooping for VLAN 1.

```
Console(config)#ip dhcp snooping vlan 1
Console(config)#
```

**RELATED COMMANDS**

ip dhcp snooping (761)
ip dhcp snooping trust (766)

## ip dhcp snooping trust

This command configures the specified interface as trusted. Use the **no** form to restore the default setting.

**SYNTAX**

[**no**] **ip dhcp snooping trust**

**DEFAULT SETTING**

All interfaces are untrusted

**COMMAND MODE**

Interface Configuration (Ethernet, Port Channel)

**COMMAND USAGE**

- A trusted interface is an interface that is configured to receive only messages from within the network. An untrusted interface is an interface that is configured to receive messages from outside the network or fire wall.

- Set all ports connected to DHCP servers within the local network or fire wall to trusted, and all other ports outside the local network or fire wall to untrusted.

- When DHCP snooping ia enabled globally using the ip dhcp snooping command, and enabled on a VLAN with ip dhcp snooping vlan command, DHCP packet filtering will be performed on any untrusted ports within the VLAN according to the default status, or as specifically configured for an interface with the **no ip dhcp snooping trust** command.

- When an untrusted port is changed to a trusted port, all the dynamic DHCP snooping bindings associated with this port are removed.

- *Additional considerations when the switch itself is a DHCP client* – The port(s) through which it submits a client request to the DHCP server must be configured as trusted.

### EXAMPLE

This example sets port 5 to untrusted.

```
Console(config)#interface ethernet 1/5
Console(config-if)#no ip dhcp snooping trust
Console(config-if)#
```

### RELATED COMMANDS

ip dhcp snooping (761)
ip dhcp snooping vlan (765)

## clear ip dhcp snooping database flash

This command removes all dynamically learned snooping entries from flash memory.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console(config)#ip dhcp snooping database flash
Console(config)#
```

## show ip dhcp snooping

This command shows the DHCP snooping configuration settings.

### Command Mode

Privileged Exec

### Example

```
Console#show ip dhcp snooping
Global DHCP Snooping status: disable
DHCP Snooping Information Option Status: disable
DHCP Snooping Information Policy: replace
DHCP Snooping is configured on the following VLANs:
1
Verify Source Mac-Address: enable
Interface        Trusted
----------       ----------
Eth 1/1          No
Eth 1/2          No
Eth 1/3          No
Eth 1/4          No
Eth 1/5          Yes
.
.
.
```

## show ip dhcp snooping binding

This command shows the DHCP snooping binding table entries.

### Command Mode

Privileged Exec

### Example

```
Console#show ip dhcp snooping binding
MacAddress        IpAddress       Lease(sec) Type                 VLAN Interface
----------------- --------------- ---------- -------------------- ---- ------
11-22-33-44-55-66 192.168.0.99             0 Dynamic-DHCPSNP         1 Eth 1/5
Console#
```

# IP SOURCE GUARD

IP Source Guard is a security feature that filters IP traffic on network interfaces based on manually configured entries in the IP Source Guard table, or dynamic entries in the DHCP Snooping table when enabled (see "DHCP Snooping" on page 761). IP source guard can be used to prevent traffic attacks caused when a host tries to use the IP address of a neighbor to access the network. This section describes commands used to configure IP Source Guard.

**Table 7: IP Source Guard Commands**

| Command | Function | Mode |
|---|---|---|
| ip source-guard binding | Adds a static address to the source-guard binding table | GC |
| ip source-guard | Configures the switch to filter inbound traffic based on source IP address, or source IP address and corresponding MAC address | IC |
| ip source-guard max-binding | Sets the maximum number of entries that can be bound to an interface | IC |
| show ip source-guard | Shows whether source guard is enabled or disabled on each interface | PE |
| show ip source-guard binding | Shows the source guard binding table | PE |

## ip source-guard binding

This command adds a static address to the source-guard binding table. Use the **no** form to remove a static entry.

### SYNTAX

**ip source-guard binding** *mac-address* **vlan** *vlan-id ip-address interface*

**no ip source-guard binding** *mac-address* **vlan** *vlan-id*

*mac-address* - A valid unicast MAC address.

*vlan-id* - ID of a configured VLAN (Range: 1-4093)

*ip-address* - A valid unicast IP address, including classful types A, B or C.

*interface* - Specifies a port interface.

**ethernet** *unit*/*port*

*unit* - This is unit 1.

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

### DEFAULT SETTING

No configured entries

### COMMAND MODE

Global Configuration

### Command Usage

- Table entries include a MAC address, IP address, lease time, entry type (Static-IP-SG-Binding, Dynamic-DHCP-Binding), VLAN identifier, and port identifier.

- All static entries are configured with an infinite lease time, which is indicated with a value of zero by the show ip source-guard command (page 772).

- When source guard is enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping, or static addresses configured in the source guard binding table with this command.

- Static bindings are processed as follows:

  - If there is no entry with same VLAN ID and MAC address, a new entry is added to binding table using the type of static IP source guard binding.

  - If there is an entry with same VLAN ID and MAC address, and the type of entry is static IP source guard binding, then the new entry will replace the old one.

  - If there is an entry with same VLAN ID and MAC address, and the type of the entry is dynamic DHCP snooping binding, then the new entry will replace the old one and the entry type will be changed to static IP source guard binding.

### Example

This example configures a static source-guard binding on port 5.

```
Console(config)#ip source-guard binding 11-22-33-44-55-66 vlan 1 192.168.0.99 interface ethernet 1/5
Console(config-if)#
```

### Related Commands

ip source-guard (770)
ip dhcp snooping (761)
ip dhcp snooping vlan (765)

## ip source-guard

This command configures the switch to filter inbound traffic based source IP address, or source IP address and corresponding MAC address. Use the **no** form to disable this function.

### Syntax

**ip source-guard** {**sip** | **sip-mac**}

**no ip source-guard**

**sip** - Filters traffic based on IP addresses stored in the binding table.

**sip-mac** - Filters traffic based on IP addresses and corresponding MAC addresses stored in the binding table.

### Default Setting

Disabled

### Command Mode

Interface Configuration (Ethernet)

### Command Usage

- Source guard is used to filter traffic on an insecure port which receives messages from outside the network or fire wall, and therefore may be subject to traffic attacks caused by a host trying to use the IP address of a neighbor.

- Setting source guard mode to “sip” or “sip-mac” enables this function on the selected port. Use the “sip” option to check the VLAN ID, source IP address, and port number against all entries in the binding table. Use the “sip-mac” option to check these same parameters, plus the source MAC address. Use the **no ip source guard** command to disable this function on the selected port.

- When enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping, or static addresses configured in the source guard binding table.

- Table entries include a MAC address, IP address, lease time, entry type (Static-IP-SG-Binding, Dynamic-DHCP-Binding, VLAN identifier, and port identifier.

- Static addresses entered in the source guard binding table with the ip source-guard binding command (page 769) are automatically configured with an infinite lease time. Dynamic entries learned via DHCP snooping are configured by the DHCP server itself.

- If the IP source guard is enabled, an inbound packet’s IP address (sip option) or both its IP address and corresponding MAC address (sip-mac option) will be checked against the binding table. If no matching entry is found, the packet will be dropped.

- Filtering rules are implemented as follows:

  - If DHCP snooping is disabled (see page 761), IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the sip-mac option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, the packet will be forwarded.

  - If the DHCP snooping is enabled, IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the sip-mac option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, or dynamic DHCP snooping binding, the packet will be forwarded.

  - If IP source guard if enabled on an interface for which IP source bindings (dynamically learned via DHCP snooping or manually configured) are not yet configured, the switch will drop all IP traffic on that port, except for DHCP packets.

  - Only unicast addresses are accepted for static bindings.

### Example

This example enables IP source guard on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard sip
Console(config-if)#
```

#### RELATED COMMANDS

ip source-guard binding (769)
ip dhcp snooping (761)
ip dhcp snooping vlan (765)

### ip source-guard max-binding

This command sets the maximum number of entries that can be bound to an interface. Use the **no** form to restore the default setting.

#### SYNTAX

**ip source-guard max-binding** *number*

**no ip source-guard max-binding**

*number* - The maximum number of IP addresses that can be mapped to an interface in the binding table. (Range: 1-5)

#### DEFAULT SETTING

5

#### COMMAND MODE

Interface Configuration (Ethernet)

#### COMMAND USAGE

- This command sets the maximum number of address entries that can be mapped to an interface in the binding table, including both dynamic entries discovered by DHCP snooping and static entries set by the ip source-guard command.

#### EXAMPLE

This example sets the maximum number of allowed entries in the binding table for port 5 to one entry.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard max-binding 1
Console(config-if)#
```

### show ip source-guard

This command shows whether source guard is enabled or disabled on each interface.

#### COMMAND MODE

Privileged Exec

#### EXAMPLE

```
Console#show ip source-guard
Interface   Filter-type   Max-binding
```

```
---------   -----------   -----------
Eth 1/1     DISABLED              5
Eth 1/2     DISABLED              5
Eth 1/3     DISABLED              5
Eth 1/4     DISABLED              5
Eth 1/5     SIP             1
Eth 1/6     DISABLED              5
:
```

### show ip source-guard binding

This command shows the source guard binding table.

**SYNTAX**

**show ip source-guard binding** [**dhcp-snooping** | **static**]

**dhcp-snooping** - Shows dynamic entries configured with DHCP Snooping commands (see page 761)

**static** - Shows static entries configured with the ip source-guard binding command (see page 769).

**COMMAND MODE**

Privileged Exec

**EXAMPLE**

```
Console#show ip source-guard binding
MacAddress        IpAddress       Lease(sec) Type                 VLAN Interface
----------------- --------------- ---------- -------------------- ---- --------
11-22-33-44-55-66 192.168.0.99            0 Static                  1 Eth 1/5
Console#
```

## ARP INSPECTION

ARP Inspection validates the MAC-to-IP address bindings in Address Resolution Protocol (ARP) packets. It protects against ARP traffic with invalid address bindings, which forms the basis for certain “man-in-the-middle” attacks. This is accomplished by intercepting all ARP requests and responses and verifying each of these packets before the local ARP cache is updated or the packet is forwarded to the appropriate destination, dropping any invalid ARP packets.

ARP Inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database – the DHCP snooping binding database. ARP Inspection can also validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured IP addresses.

This section describes commands used to configure ARP Inspection.

**Table 8: ARP Inspection Commands**

| Command | Function | Mode |
|---|---|---|
| ip arp inspection | Enables ARP Inspection globally on the switch | GC |
| ip arp inspection filter | Specifies an ARP ACL to apply to one or more VLANs | GC |
| ip arp inspection log-buffer logs | Sets the maximum number of entries saved in a log message, and the rate at these messages are sent | GC |
| ip arp inspection validate | Specifies additional validation of address components in an ARP packet | GC |
| ip arp inspection vlan | Enables ARP Inspection for a specified VLAN or range of VLANs | GC |
| ip arp inspection limit | Sets a rate limit for the ARP packets received on a port | IC |
| ip arp inspection trust | Sets a port as trusted, and thus exempted from ARP Inspection | IC |
| show ip arp inspection configuration | Displays the global configuration settings for ARP Inspection | PE |
| show ip arp inspection interface | Shows the trust status and inspection rate limit for ports | PE |
| show ip arp inspection log | Shows information about entries stored in the log, including the associated VLAN, port, and address components | PE |
| show ip arp inspection statistics | Shows statistics about the number of ARP packets processed, or dropped for various reasons | PE |
| show ip arp inspection vlan | Shows configuration setting for VLANs, including ARP Inspection status, the ARP ACL name, and if the DHCP Snooping database is used after ACL validation is completed | PE |

## ip arp inspection

This command enables ARP Inspection globally on the switch. Use the **no** form to disable this function.

### SYNTAX

[**no**] **ip arp inspection**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- When ARP Inspection is enabled globally with this command, it becomes active only on those VLANs where it has been enabled with the ip arp inspection vlan command.

- When ARP Inspection is enabled globally and enabled on selected VLANs, all ARP request and reply packets on those VLANs are redirected to the CPU and their switching is handled by the ARP Inspection engine.

■When ARP Inspection is disabled globally, it becomes inactive for all VLANs, including those where ARP Inspection is enabled.

■When ARP Inspection is disabled, all ARP request and reply packets bypass the ARP Inspection engine and their manner of switching matches that of all other packets.

■Disabling and then re-enabling global ARP Inspection will not affect the ARP Inspection configuration for any VLANs.

■When ARP Inspection is disabled globally, it is still possible to configure ARP Inspection for individual VLANs. These configuration changes will only become active after ARP Inspection is globally enabled again.

### EXAMPLE

```
Console(config)#ip arp inspection
Console(config)#
```

## ip arp inspection filter

This command specifies an ARP ACL to apply to one or more VLANs. Use the **no** form to remove an ACL binding.

### SYNTAX

**ip arp inspection filter** *arp-acl-name* **vlan** {*vlan-id* | *vlan-range*} [**static**]

arp-acl-name - Name of an ARP ACL. (Maximum length: 16 characters)

*vlan-id* - VLAN ID. (Range: 1-4093)

*vlan-range* - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

**static** - ARP packets are only validated against the specified ACL, address bindings in the DHCP snooping database is not checked.

### DEFAULT SETTING

ARP ACLs are not bound to any VLAN

Static mode is not enabled

### COMMAND MODE

Global Configuration

### COMMAND USAGE

■ARP ACLs are configured with the commands described on page 291.

■If static mode is enabled, the switch compares ARP packets to the specified ARP ACLs. Packets matching an IP-to-MAC address binding in a permit or deny rule are processed accordingly. Packets not matching any of the ACL rules are dropped. Address bindings in the DHCP snooping database are not checked.

- If static mode is not enabled, packets are first validated against the specified ARP ACL. Packets matching a deny rule are dropped. All remaining packets are validated against the address bindings in the DHCP snooping database.

### Example

```
Console(config)#ip arp inspection filter sales vlan 1
Console(config)#
```

## ip arp inspection log-buffer logs

This command sets the maximum number of entries saved in a log message, and the rate at which these messages are sent. Use the **no** form to restore the default settings.

### Syntax

**ip arp inspection log-buffer logs** *message-number* **interval** *seconds*

**no ip arp inspection log-buffer logs**

*message-number* - The maximum number of entries saved in a log message. (Range: 0-256, where 0 means no events are saved)

*seconds* - The interval at which log messages are sent. (Range: 0-86400)

### Default Setting

Message Number: 5
Interval: 1 second

### Command Mode

Global Configuration

### Command Usage

- ARP Inspection must be enabled with the ip arp inspection command before this command will be accepted by the switch.
- By default, logging is active for ARP Inspection, and cannot be disabled.
- When the switch drops a packet, it places an entry in the log buffer. Each entry contains flow information, such as the receiving VLAN, the port number, the source and destination IP addresses, and the source and destination MAC addresses.
- If multiple, identical invalid ARP packets are received consecutively on the same VLAN, then the logging facility will only generate one entry in the log buffer and one corresponding system message.
- The maximum number of entries that can be stored in the log buffer is determined by the *message-number* parameter. If the log buffer fills up before a message is sent, the oldest entry will be replaced with the newest one.

■The switch generates a system message on a rate-controlled basis determined by the *seconds* values. After the system message is generated, all entries are cleared from the log buffer.

**EXAMPLE**

```
Console(config)#ip arp inspection log-buffer logs 1 interval 10
Console(config)#
```

## ip arp inspection validate

This command specifies additional validation of address components in an ARP packet. Use the **no** form to restore the default setting.

**SYNTAX**

**ip arp inspection validate** {**dst-mac** [**ip**] [**src-mac**] | **ip** [**src-mac**] | **src-mac**}

**no ip arp inspection validate**

**dst-mac** - Checks the destination MAC address in the Ethernet header against the target MAC address in the ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

**ip** - Checks the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, while target IP addresses are checked only in ARP responses.

**src-mac** - Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

**DEFAULT SETTING**
No additional validation is performed

**COMMAND MODE**
Global Configuration

**COMMAND USAGE**
By default, ARP Inspection only checks the IP-to-MAC address bindings specified in an ARP ACL or in the DHCP Snooping database.

**EXAMPLE**

```
Console(config)#ip arp inspection validate dst-mac
Console(config)#
```

## ip arp inspection vlan

This command enables ARP Inspection for a specified VLAN or range of VLANs. Use the **no** form to disable this function.

#### Syntax

[**no**] **ip arp inspection vlan** {*vlan-id* | *vlan-range*}

*vlan-id* - VLAN ID. (Range: 1-4093)

*vlan-range* - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

#### Default Setting

Disabled on all VLANs

#### Command Mode

Global Configuration

#### Command Usage

- When ARP Inspection is enabled globally with the ip arp inspection command, it becomes active only on those VLANs where it has been enabled with this command.
- When ARP Inspection is enabled globally and enabled on selected VLANs, all ARP request and reply packets on those VLANs are redirected to the CPU and their switching is handled by the ARP Inspection engine.
- When ARP Inspection is disabled globally, it becomes inactive for all VLANs, including those where ARP Inspection is enabled.
- When ARP Inspection is disabled, all ARP request and reply packets bypass the ARP Inspection engine and their manner of switching matches that of all other packets.
- Disabling and then re-enabling global ARP Inspection will not affect the ARP Inspection configuration for any VLANs.
- When ARP Inspection is disabled globally, it is still possible to configure ARP Inspection for individual VLANs. These configuration changes will only become active after ARP Inspection is globally enabled again.

#### Example

```
Console(config)#ip arp inspection vlan 1,2
Console(config)#
```

### ip arp inspection limit

This command sets a rate limit for the ARP packets received on a port. Use the **no** form to restore the default setting.

#### Syntax

**ip arp inspection limit** {**rate** *pps* | **none**}

**no ip arp inspection limit**

*pps* - The maximum number of ARP packets that can be processed by the CPU per second. (Range: 0-2048, where 0 means that no ARP packets can be forwarded)

**none** - There is no limit on the number of ARP packets that can be processed by the CPU.

**DEFAULT SETTING**
15

**COMMAND MODE**
Interface Configuration (Port)

**COMMAND USAGE**

- This command only applies to untrusted ports.
- When the rate of incoming ARP packets exceeds the configured limit, the switch drops all ARP packets in excess of the limit.

**EXAMPLE**

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip arp inspection limit 150
Console(config-if)#
```

## ip arp inspection trust

This command sets a port as trusted, and thus exempted from ARP Inspection. Use the **no** form to restore the default setting.

**SYNTAX**

[**no**] **ip arp inspection trust**

**DEFAULT SETTING**
Untrusted

**COMMAND MODE**
Interface Configuration (Port)

**COMMAND USAGE**
Packets arriving on untrusted ports are subject to any configured ARP Inspection and additional validation checks. Packets arriving on trusted ports bypass all of these checks, and are forwarded according to normal switching rules.

**EXAMPLE**

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip arp inspection trust
Console(config-if)#
```

## show ip arp inspection configuration

This command displays the global configuration settings for ARP Inspection.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show ip arp inspection configuration

ARP inspection global information:

Global IP ARP Inspection status : disabled
Log Message Interval           : 10 s
Log Message Number             : 1
Need Additional Validation(s)  : Yes
Additional Validation Type     : Destination MAC address
Console#
```

## show ip arp inspection interface

This command shows the trust status and ARP Inspection rate limit for ports.

### SYNTAX

**show ip arp inspection interface** [*interface*]

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show ip arp inspection interface ethernet 1/1

Port Number       Trust Status          Limit Rate (pps)
-------------   --------------------   -------------------------------
Eth 1/1           trusted                   150
Console#
```

## show ip arp inspection log

This command shows information about entries stored in the log, including the associated VLAN, port, and address components.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show ip arp inspection log
Total log entries number is 1

Num VLAN Port Src IP Address  Dst IP Address  Src MAC Address  Dst MAC Address
--- ---- ---- --------------  --------------  ---------------  --------------
```

```
1   1     11  192.168.2.2     192.168.2.1     00-04-E2-A0-E2-7C FF-FF-FF-FF-FF-FF
Console#
```

## show ip arp inspection statistics

This command shows statistics about the number of ARP packets processed, or dropped for various reasons.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show ip arp inspection log
Total log entries number is 1

Num VLAN Port Src IP Address  Dst IP Address  Src MAC Address  Dst MAC Address
--- ---- ---- --------------  --------------  ---------------  -----------

Console#show ip arp inspection statistics

ARP packets received before rate limit                          : 150
ARP packets dropped due to rate limt                            : 5
Total ARP packets processed by ARP Inspection                   : 150
ARP packets dropped by additional validation (source MAC address)     : 0
ARP packets dropped by additional validation (destination MAC address): 0
ARP packets dropped by additional validation (IP address)             : 0
ARP packets dropped by ARP ACLs                                 : 0
ARP packets dropped by DHCP snooping                            : 0

Console#
```

## show ip arp inspection vlan

This command shows the configuration settings for VLANs, including ARP Inspection status, the ARP ACL name, and if the DHCP Snooping database is used after ARP ACL validation is completed.

### SYNTAX

**show ip arp inspection vlan** [*vlan-id* **|** *vlan-range*]

*vlan-id* - VLAN ID. (Range: 1-4093)

*vlan-range* - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show ip arp inspection vlan 1

VLAN ID     DAI Status          ACL Name            ACL Status
--------   ---------------   --------------------   --------------------
1          disabled            sales               static
Console#
```

# 31 ACCESS CONTROL LISTS

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

**Table 1: Access Control List Commands**

| Command Group | Function |
|---|---|
| IPv4 ACLS | Configures ACLs based on IPv4 addresses, TCP/UDP port number, protocol type, and TCP control code |
| IPv6 ACLs | Configures ACLs based on IPv6 addresses or DSCP traffic class |
| MAC ACLs | Configures ACLs based on hardware addresses, packet format, and Ethernet type |
| ARP ACLs | Configures ACLs based on ARP messages addresses |
| ACL Information | Displays ACLs and associated rules; shows ACLs assigned to each port |

## IPv4 ACLs

The commands in this section configure ACLs based on IPv4 addresses, TCP/UDP port number, protocol type, and TCP control code. To configure IPv4 ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports.

**Table 2: IPv4 ACL Commands**

| Command | Function | Mode |
|---|---|---|
| access-list ip | Creates an IP ACL and enters configuration mode for standard or extended IPv4 ACLs | GC |
| permit, deny | Filters packets matching a specified source IPv4 address | IPv4-STD-ACL |
| permit, deny | Filters packets meeting the specified criteria, including source and destination IPv4 address, TCP/UDP port number, protocol type, and TCP control code | IPv4-EXT-ACL |
| ip access-group | Binds an IPv4 ACL to a port | IC |
| show ip access-group | Shows port assignments for IPv4 ACLs | PE |
| show ip access-list | Displays the rules for configured IPv4 ACLs | PE |

## access-list ip

This command adds an IP access list and enters configuration mode for standard or extended IPv4 ACLs. Use the **no** form to remove the specified ACL.

### SYNTAX

[**no**] **access-list ip** {**standard** | **extended**} *acl-name*

**standard** – Specifies an ACL that filters packets based on the source IP address.

**extended** – Specifies an ACL that filters packets based on the source or destination IP address, and other more specific criteria.

*acl-name* – Name of the ACL. (Maximum length: 16 characters, no spaces or other special characters)

### DEFAULT SETTING

None

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 128 rules.

### EXAMPLE

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

### RELATED COMMANDS

permit, deny (785)
ip access-group (788)
show ip access-list (789)

## **permit**, **deny** (Standard IP ACL)

This command adds a rule to a Standard IPv4 ACL. The rule sets a filter condition for packets emanating from the specified source. Use the **no** form to remove a rule.

### SYNTAX

{**permit** | **deny**} {**any** | *source bitmask* | **host** *source*}
[**time-range** *time-range-name*]

**no** {**permit** | **deny**} {**any** | *source bitmask* | **host** *source*}

**any** – Any source IP address.

*source* – Source IP address.

*bitmask* – Decimal number representing the address bits to match.

**host** – Keyword followed by a specific IP address.

*time-range-name* - Name of the time range.
(Range: 1-30 characters)

### DEFAULT SETTING

None

### COMMAND MODE

Standard IPv4 ACL

### COMMAND USAGE

- New rules are appended to the end of the list.
- Address bit masks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

### EXAMPLE

This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

```
Console(config-std-acl)#permit host 10.1.1.21
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

### RELATED COMMANDS

access-list ip (784)
Time Range (654)

**permit**, **deny** (Extended IPv4 ACL)

This command adds a rule to an Extended IPv4 ACL. The rule sets a filter condition for packets with specific source or destination IP addresses, protocol types, source or destination protocol ports, or TCP control codes. Use the **no** form to remove a rule.

### SYNTAX

{**permit** | **deny**} [*protocol-number* | **udp**]
{**any** | *source address-bitmask* | **host** *source*}
{**any** | *destination address-bitmask* | **host** *destination*}
[**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*]
[**source**-port *sport* [*bitmask*]]
[**destination**-port *dport* [*port-bitmask*]]
[**time-range** *time-range-name*]

**no** {**permit** | **deny**} [*protocol-number* | **udp**]
{**any** | *source address-bitmask* | **host** *source*}
{**any** | *destination address-bitmask* | **host** *destination*}
[**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*]
[**source**-port *sport* [*bitmask*]]
[**destination**-port *dport* [*port-bitmask*]]

{**permit** | **deny**} **tcp**
{**any** | *source address-bitmask* | **host** *source*}
{**any** | *destination address-bitmask* | **host** *destination*}
[**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*]
[**source-port** *sport* [*bitmask*]]
[**destination-port** *dport* [*port-bitmask*]]
[**control-flag** *control-flags flag-bitmask*]
[**time-range** *time-range-name*]

**no** {**permit** | **deny**} **tcp**
{**any** | *source address-bitmask* | **host** *source*}
{**any** | *destination address-bitmask* | **host** *destination*}
[**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*]
[**source-port** *sport* [*bitmask*]]
[**destination-port** *dport* [*port-bitmask*]]
[**control-flag** *control-flags flag-bitmask*]

*protocol-number* – A specific protocol number. (Range: 0-255)

*source* – Source IP address.

*destination* – Destination IP address.

*address-bitmask* – Decimal number representing the address bits to match.

**host** – Keyword followed by a specific IP address.

*precedence* – IP precedence level. (Range: 0-7)

*tos* – Type of Service level. (Range: 0-15)

*dscp* – DSCP priority level. (Range: 0-63)

*sport* – Protocol[1] source port number. (Range: 0-65535)

*dport* – Protocol[1] destination port number. (Range: 0-65535)

*port-bitmask* – Decimal number representing the port bits to match. (Range: 0-65535)

1. Includes TCP, UDP or other protocol types.

*control-flags* – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)

*flag-bitmask* – Decimal number representing the code bits to match.

*time-range-name* - Name of the time range.
(Range: 1-30 characters)

**DEFAULT SETTING**
None

**COMMAND MODE**
Extended IPv4 ACL

**COMMAND USAGE**

■ All new rules are appended to the end of the list.

■ Address bit masks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The bit mask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

■ You can specify both Precedence and ToS in the same rule. However, if DSCP is used, then neither Precedence nor ToS can be specified.

■ The control-code bitmask is a decimal number (representing an equivalent bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit “1” means to match a bit and “0” means to ignore a bit. The following bits may be specified:

- 1 (fin) – Finish
- 2 (syn) – Synchronize
- 4 (rst) – Reset
- 8 (psh) – Push
- 16 (ack) – Acknowledgement
- 32 (urg) – Urgent pointer

For example, use the code value and mask below to catch packets with the following flags set:

- SYN flag valid, use “control-code 2 2”
- Both SYN and ACK valid, use “control-code 18 18”
- SYN valid and ACK invalid, use “control-code 2 18”

**EXAMPLE**
This example accepts any incoming packets if the source address is within subnet 10.7.1.x. For example, if the rule is matched; i.e., the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any
Console(config-ext-acl)#
```

This allows TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (i.e., HTTP).

```
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any destination-port 80
Console(config-ext-acl)#
```

This permits all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to “SYN.”

```
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any  control-flag 2 2
Console(config-ext-acl)#
```

**RELATED COMMANDS**

access-list ip (784)
Time Range (654)

## ip access-group

This command binds an IPv4 ACL to a port. Use the **no** form to remove the port.

**SYNTAX**

**ip access-group** *acl-name* **in** [**time-range** *time-range-name*]

**no ip access-group** *acl-name* **in**

*acl-name* – Name of the ACL. (Maximum length: 16 characters)

**in** – Indicates that this list applies to ingress packets.

*time-range-name* - Name of the time range.
(Range: 1-30 characters)

**DEFAULT SETTING**

None

**COMMAND MODE**

Interface Configuration (Ethernet)

**COMMAND USAGE**

- Only one ACL can be bound to a port.
- If an ACL is already bound to a port and you bind a different ACL to it, the switch will replace the old binding with the new one.

**EXAMPLE**

```
Console(config)#int eth 1/2
Console(config-if)#ip access-group david in
Console(config-if)#
```

#### RELATED COMMANDS

show ip access-list (789)
Time Range (654)

### show ip access-group

This command shows the ports assigned to IP ACLs.

#### COMMAND MODE

Privileged Exec

#### EXAMPLE

```
Console#show ip access-group
Interface ethernet 1/2
 IP access-list david in
Console#
```

#### RELATED COMMANDS

ip access-group (788)

### show ip access-list

This command displays the rules for configured IPv4 ACLs.

#### SYNTAX

**show ip access-list** {**standard** | **extended**} [*acl-name*]

**standard** – Specifies a standard IP ACL.

**extended** – Specifies an extended IP ACL.

*acl-name* – Name of the ACL. (Maximum length: 16 characters)

#### COMMAND MODE

Privileged Exec

#### EXAMPLE

```
Console#show ip access-list standard
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 255.255.15.0
Console#
```

#### RELATED COMMANDS

permit, deny (785)
ip access-group (788)

## IPv6 ACLs

The commands in this section configure ACLs based on IPv6 address, DSCP traffic class, next header type, or flow label. To configure IPv6 ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports.

**Table 3: IPv4 ACL Commands**

| Command | Function | Mode |
|---|---|---|
| access-list ipv6 | Creates an IPv6 ACL and enters configuration mode for standard or extended IPv6 ACLs | GC |
| permit, deny | Filters packets matching a specified source IPv6 address | IPv6-STD-ACL |
| permit, deny | Filters packets meeting the specified criteria, including destination IPv6 address, DSCP traffic class, next header type, and flow label | IPv6- EXT-ACL |
| show ipv6 access-list | Displays the rules for configured IPv6 ACLs | PE |
| ipv6 access-group | Adds a port to an IPv6 ACL | IC |
| show ipv6 access-group | Shows port assignments for IPv6 ACLs | PE |

### access-list ipv6

This command adds an IP access list and enters configuration mode for standard or extended IPv6 ACLs. Use the **no** form to remove the specified ACL.

#### SYNTAX

[**no**] **access-list ipv6** {**standard** | **extended**} *acl-name*

**standard** – Specifies an ACL that filters packets based on the source IP address.

**extended** – Specifies an ACL that filters packets based on the destination IP address, and other more specific criteria.

*acl-name* – Name of the ACL. (Maximum length: 16 characters)

#### DEFAULT SETTING

None

#### COMMAND MODE

Global Configuration

#### COMMAND USAGE

- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 128 rules.

### EXAMPLE

```
Console(config)#access-list ipv6 standard david
Console(config-std-ipv6-acl)#
```

### RELATED COMMANDS

permit, deny (Standard IPv6 ACL) (791)
permit, deny (Extended IPv6 ACL) (792)
ipv6 access-group (794)
show ipv6 access-list (794)

## **permit**, **deny** (Standard IPv6 ACL)

This command adds a rule to a Standard IPv6 ACL. The rule sets a filter condition for packets emanating from the specified source. Use the **no** form to remove a rule.

### SYNTAX

{**permit** | **deny**} {**any** | **host** *source-ipv6-address* |
*source-ipv6-address*[/*prefix-length*]}
[**time-range** *time-range-name*]

**no** {**permit** | **deny**} {**any** | **host** *source-ipv6-address* |
*source-ipv6-address*[/*prefix-length*]}

**any** – Any source IP address.

**host** – Keyword followed by a specific IP address.

*source-ipv6-address* - An IPv6 source address or network class. The address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

*prefix-length* - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix; i.e., the network portion of the address. (Range: 0-128)

*time-range-name* - Name of the time range.
(Range: 1-30 characters)

### DEFAULT SETTING

None

### COMMAND MODE

Standard IPv6 ACL

### COMMAND USAGE

New rules are appended to the end of the list.

### EXAMPLE

This example configures one permit rule for the specific address 2009:DB9:2229::79 and another rule for the addresses with the network prefix 2009:DB9:2229:5::/64.

```
Console(config-std-ipv6-acl)#permit host 2009:DB9:2229::79
Console(config-std-ipv6-acl)#permit 2009:DB9:2229:5::/64
Console(config-std-ipv6-acl)#
```

### RELATED COMMANDS

access-list ipv6 (790)
Time Range (654)

## **permit**, **deny** (Extended IPv6 ACL)

This command adds a rule to an Extended IPv6 ACL. The rule sets a filter condition for packets with specific destination IP addresses, next header type, or flow label. Use the **no** form to remove a rule.

### SYNTAX

[**no**] {**permit** | **deny**}
{**any** | *destination-ipv6-address*[*/prefix-length*]}
[**dscp** *dscp*] [**flow-label** *flow-label*] [**next-header** *next-header*] [**time-range** *time-range-name*]

**any** – Any IP address (an abbreviation for the IPv6 prefix ::/0).

*destination-ipv6-address* - An IPv6 destination address or network class. The address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (The switch only checks the first 64 bits of the destination address.)

*prefix-length* - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix; i.e., the network portion of the address. (Range: 0-128 for source prefix, 0-8 for destination prefix)

*dscp* – DSCP traffic class. (Range: 0-63)

*flow-label* – A label for packets belonging to a particular traffic “flow” for which the sender requests special handling by IPv6 routers, such as non-default quality of service or “real-time” service (see RFC 2460). (Range: 0-16777215)

*next-header* – Identifies the type of header immediately following the IPv6 header. (Range: 0-255)

*time-range-name* - Name of the time range.
(Range: 1-30 characters)

### DEFAULT SETTING

None

### COMMAND MODE

Extended IPv6 ACL

### COMMAND USAGE

■All new rules are appended to the end of the list.

■A flow label is assigned to a flow by the flow's source node. New flow labels must be chosen pseudo-randomly and uniformly from the range 1 to FFFFF hexadecimal. The purpose of the random allocation is to make any set of bits within the Flow Label field suitable for use as a hash key by routers, for looking up the state associated with the flow.

A flow identifies a sequence of packets sent from a particular source to a particular (unicast or multicast) destination for which the source desires special handling by the intervening routers. The nature of that special handling might be conveyed to the routers by a control protocol, such as a resource reservation protocol, or by information within the flow's packets themselves, e.g., in a hop-by-hop option. A flow is uniquely identified by the combination of a source address and a non-zero flow label. Packets that do not belong to a flow carry a flow label of zero.

Hosts or routers that do not support the functions specified by the flow label must set the field to zero when originating a packet, pass the field on unchanged when forwarding a packet, and ignore the field when receiving a packet.

■Optional internet-layer information is encoded in separate headers that may be placed between the IPv6 header and the upper-layer header in a packet. There are a small number of such extension headers, each identified by a distinct Next Header value. IPv6 supports the values defined for the IPv4 Protocol field in RFC 1700, including these commonly used headers:

| | | |
|---|---|---|
| 0 | : Hop-by-Hop Options | (RFC 2460) |
| 6 | : TCP Upper-layer Header | (RFC 1700) |
| 17 | : UDP Upper-layer Header | (RFC 1700) |
| 43 | : Routing | (RFC 2460) |
| 44 | : Fragment | (RFC 2460) |
| 51 | : Authentication | (RFC 2402) |
| 50 | : Encapsulating Security Payload | (RFC 2406) |
| 60 | : Destination Options | (RFC 2460) |

### EXAMPLE

This example accepts any incoming packets if the destination address is 2009:DB9:2229::79/8.

```
Console(config-ext-ipv6-acl)#permit 2009:DB9:2229::79/8
Console(config-ext-ipv6-acl)#
```

This allows packets to any destination address when the DSCP value is 5.

```
Console(config-ext-ipv6-acl)#permit any dscp 5
Console(config-ext-ipv6-acl)#
```

This allows any packets sent to the destination 2009:DB9:2229::79/48 when the flow label is 43.”

```
Console(config-ext-ipv6-acl)#permit 2009:DB9:2229::79/48 flow-label 43
Console(config-ext-ipv6-acl)#
```

#### RELATED COMMANDS

access-list ipv6 (790)
Time Range (654)

### show ipv6 access-list

This command displays the rules for configured IPv6 ACLs.

#### SYNTAX

**show ipv6 access-list** {**standard** | **extended**} [*acl-name*]

**standard** – Specifies a standard IPv6 ACL.

**extended** – Specifies an extended IPv6 ACL.

*acl-name* – Name of the ACL. (Maximum length: 16 characters)

#### COMMAND MODE

Privileged Exec

#### EXAMPLE

```
Console#show ipv6 access-list standard
IPv6 standard access-list david:
  permit host 2009:DB9:2229::79
  permit 2009:DB9:2229:5::/64
Console#
```

#### RELATED COMMANDS

permit, deny (Standard IPv6 ACL) (791)
permit, deny (Extended IPv6 ACL) (792)
ipv6 access-group (794)

### ipv6 access-group

This command binds a port to an IPv6 ACL. Use the **no** form to remove the port.

#### SYNTAX

**ipv6 access-group** *acl-name* **in** [**time-range** *time-range-name*]

**no ipv6 access-group** *acl-name* **in**

*acl-name* – Name of the ACL. (Maximum length: 16 characters)

**in** – Indicates that this list applies to ingress packets.

*time-range-name* - Name of the time range.
(Range: 1-30 characters)

#### DEFAULT SETTING

None

**COMMAND MODE**
Interface Configuration (Ethernet)

**COMMAND USAGE**

- A port can only be bound to one ACL.
- If a port is already bound to an ACL and you bind it to a different ACL, the switch will replace the old binding with the new one.
- IPv6 ACLs can only be applied to ingress packets.

**EXAMPLE**

```
Console(config)#interface ethernet 1/2
Console(config-if)#ipv6 access-group standard david in
Console(config-if)#
```

**RELATED COMMANDS**
show ipv6 access-list (794)
Time Range (654)

## show ipv6 access-group

This command shows the ports assigned to IPv6 ACLs.

**COMMAND MODE**
Privileged Exec

**EXAMPLE**

```
Console#show ipv6 access-group
Interface ethernet 1/2
 IPv6 access-list david in
Console#
```

**RELATED COMMANDS**
ipv6 access-group (794)

# MAC ACLS

The commands in this section configure ACLs based on hardware addresses, packet format, and Ethernet type. To configure MAC ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports.

**Table 4: MAC ACL Commands**

| Command | Function | Mode |
|---|---|---|
| access-list mac | Creates a MAC ACL and enters configuration mode | GC |
| permit, deny | Filters packets matching a specified source and destination address, packet format, and Ethernet type | MAC-ACL |
| mac access-group | Binds a MAC ACL to a port | IC |
| show mac access-group | Shows port assignments for MAC ACLs | PE |
| show mac access-list | Displays the rules for configured MAC ACLs | PE |

## access-list mac

This command adds a MAC access list and enters MAC ACL configuration mode. Use the **no** form to remove the specified ACL.

### SYNTAX

[**no**] **access-list mac** *acl-name*

*acl-name* – Name of the ACL. (Maximum length: 16 characters, no spaces or other special characters)

### DEFAULT SETTING

None

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 128 rules.

### EXAMPLE

```
Console(config)#access-list mac jerry
Console(config-mac-acl)#
```

**RELATED COMMANDS**

permit, deny (797)
mac access-group (799)
show mac access-list (800)

**permit, deny (MAC ACL)**

This command adds a rule to a MAC ACL. The rule filters packets matching a specified MAC source or destination address (i.e., physical layer address), or Ethernet protocol type. Use the **no** form to remove a rule.

**SYNTAX**

{**permit** | **deny**}
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*] [**ethertype** *protocol* [*protocol-bitmask*]] [**time-range** *time-range-name*]

**no** {**permit** | **deny**}
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*] [**ethertype** *protocol* [*protocol-bitmask*]]

**NOTE:** The default is for Ethernet II packets.

{**permit** | **deny**} **tagged-eth2**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*] [**ethertype** *protocol* [*protocol-bitmask*]] [**time-range** *time-range-name*]

**no** {**permit** | **deny**} **tagged-eth2**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*] [**ethertype** *protocol* [*protocol-bitmask*]]

{**permit** | **deny**} **untagged-eth2**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**ethertype** *protocol* [*protocol-bitmask*]]
[**time-range** *time-range-name*]

**no** {**permit** | **deny**} **untagged-eth2**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**ethertype** *protocol* [*protocol-bitmask*]]

{**permit** | **deny**} **tagged-802.3**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*] [**time-range** *time-range-name*]

**no** {**permit** | **deny**} **tagged-802.3**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*]

{**permit** | **deny**} **untagged-802.3**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**time-range** *time-range-name*]

**no** {**permit** | **deny**} **untagged-802.3**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}

**tagged-eth2** – Tagged Ethernet II packets.

**untagged-eth2** – Untagged Ethernet II packets.

**tagged-802.3** – Tagged Ethernet 802.3 packets.

**untagged-802.3** – Untagged Ethernet 802.3 packets.

**any** – Any MAC source or destination address.

**host** – A specific MAC address.

*source* – Source MAC address.

*destination* – Destination MAC address range with bitmask.

*address-bitmask*[2] – Bitmask for MAC address (in hexadecimal format).

*vid* – VLAN ID. (Range: 1-4093)

*vid-bitmask*[2] – VLAN bitmask. (Range: 1-4095)

*protocol* – A specific Ethernet protocol number. (Range: 600-ffff hex.)

*protocol-bitmask*[2] – Protocol bitmask.
(Range: 600-ffff hex.)

*time-range-name* - Name of the time range.
(Range: 1-30 characters)

### DEFAULT SETTING
None

### COMMAND MODE
MAC ACL

### COMMAND USAGE
■New rules are added to the end of the list.

■The **ethertype** option can only be used to filter Ethernet II formatted packets.

■A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include the following:

- 0800 - IP
- 0806 - ARP
- 8137 - IPX

### EXAMPLE
This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

2. For all bitmasks, “1” means care and “0” means ignore.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de ethertype 0800
Console(config-mac-acl)#
```

#### RELATED COMMANDS
access-list mac (796)
Time Range (654)

### mac access-group

This command binds a MAC ACL to a port. Use the **no** form to remove the port.

#### SYNTAX

**mac access-group** *acl-name* **in** [**time-range** *time-range-name*]

*acl-name* – Name of the ACL. (Maximum length: 16 characters)

**in** – Indicates that this list applies to ingress packets.

*time-range-name* - Name of the time range.
(Range: 1-30 characters)

#### DEFAULT SETTING
None

#### COMMAND MODE
Interface Configuration (Ethernet)

#### COMMAND USAGE
- Only one ACL can be bound to a port.
- If an ACL is already bound to a port and you bind a different ACL to it, the switch will replace the old binding with the new one.

#### EXAMPLE

```
Console(config)#interface ethernet 1/2
Console(config-if)#mac access-group jerry in
Console(config-if)#
```

#### RELATED COMMANDS
show mac access-list (800)
Time Range (654)

## show mac access-group

This command shows the ports assigned to MAC ACLs.

**Command Mode**

Privileged Exec

**Example**

```
Console#show mac access-group
Interface ethernet 1/5
 MAC access-list M5 in
Console#
```

**Related Commands**

mac access-group (799)

## show mac access-list

This command displays the rules for configured MAC ACLs.

**Syntax**

**show mac access-list** [*acl-name*]

*acl-name* – Name of the ACL. (Maximum length: 16 characters)

**Command Mode**

Privileged Exec

**Example**

```
Console#show mac access-list
MAC access-list jerry:
  permit any 00-e0-29-94-34-de ethertype 0800
Console#
```

**Related Commands**

permit, deny (797)
mac access-group (799)

# ARP ACLS

The commands in this section configure ACLs based on the IP or MAC address contained in ARP request and reply messages. To configure ARP ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more VLANs using the ip arp inspection vlan command.

**Table 5: ARP ACL Commands**

| Command | Function | Mode |
|---|---|---|
| access-list arp | Creates a ARP ACL and enters configuration mode | GC |
| permit, deny | Filters packets matching a specified source or destination address in ARP messages | ARP-ACL |
| show arp access-list | Displays the rules for configured ARP ACLs | PE |

## access-list arp

This command adds an ARP access list and enters ARP ACL configuration mode. Use the **no** form to remove the specified ACL.

### SYNTAX

[**no**] **access-list arp** *acl-name*

*acl-name* – Name of the ACL. (Maximum length: 16 characters)

### DEFAULT SETTING

None

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 96 rules.

### EXAMPLE

```
Console(config)#access-list arp factory
Console(config-arp-acl)#
```

### RELATED COMMANDS

permit, deny (802)
show arp access-list (803)

**permit**, **deny** (ARP ACL)

This command adds a rule to an ARP ACL. The rule filters packets matching a specified source or destination address in ARP messages. Use the **no** form to remove a rule.

**SYNTAX**

[**no**] {**permit** | **deny**}
**ip** {**any** | **host** *source-ip* | *source-ip ip-address-bitmask*}
**mac** {**any** | **host** *source-ip* | *source-ip ip-address-bitmask*} [**log**]

This form indicates either request or response packets.

[**no**] {**permit** | **deny**} **request**
**ip** {**any** | **host** *source-ip* | *source-ip ip-address-bitmask*}
**mac** {**any** | **host** *source-mac* | *source-mac mac-address-bitmask*} [**log**]

[**no**] {**permit** | **deny**} **response**
**ip** {**any** | **host** *source-ip* | *source-ip ip-address-bitmask*}
{**any** | **host** *destination-ip* | *destination-ip ip-address-bitmask*}
**mac** {**any** | **host** *source-mac* | *source-mac mac-address-bitmask*}
[**any** | **host** *destination-mac* | *destination-mac mac-address-bitmask*] [**log**]

*source-ip* – Source IP address.

*destination-ip* – Destination IP address with bitmask.

*ip-address-bitmask*[3] – IPv4 number representing the address bits to match.

*source-mac* – Source MAC address.

*destination-mac* – Destination MAC address range with bitmask.

*mac-address-bitmask*[3] – Bitmask for MAC address (in hexadecimal format).

**log** - Logs a packet when it matches the access control entry.

**DEFAULT SETTING**
None

**COMMAND MODE**
ARP ACL

**COMMAND USAGE**
New rules are added to the end of the list.

**EXAMPLE**
This rule permits packets from any source IP and MAC address to the destination subnet address 192.168.0.0.

```
Console(config-arp-acl)#$permit response ip any 192.168.0.0 255.255.0.0 mac any any
Console(config-mac-acl)#
```

**RELATED COMMANDS**
access-list arp (801)

3. For all bitmasks, binary “1” means care and “0” means ignore.

**show arp access-list** This command displays the rules for configured ARP ACLs.

### SYNTAX

**show arp access-list** [*acl-name*]

*acl-name* – Name of the ACL. (Maximum length: 16 characters)

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show arp access-list
ARP access-list factory:
  permit response ip any 192.168.0.0 255.255.0.0 mac any any
Console#
```

### RELATED COMMANDS

permit, deny (802)

## ACL INFORMATION

This section describes commands used to display ACL information.

**Table 6: ACL Information Commands**

| Command | Function | Mode |
|---|---|---|
| show access-group | Shows the ACLs assigned to each port | PE |
| show access-list | Show all ACLs and associated rules | PE |

**show access-group** This command shows the port assignments of ACLs.

### COMMAND MODE

Privileged Executive

### EXAMPLE

```
Console#show access-group
Interface ethernet 1/2
 IP access-list david
 MAC access-list jerry
Console#
```

**show access-list** This command shows all ACLs and associated rules.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show access-list
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 255.255.15.0
IP extended access-list bob:
  permit 10.7.1.1 255.255.255.0 any
  permit 192.168.1.0 255.255.255.0 any destination-port 80 80
  permit 192.168.1.0 255.255.255.0 any protocol tcp control-code 2 2
MAC access-list jerry:
  permit any host 00-30-29-94-34-de ethertype 800 800
  permit any any
Console#
```

# 32 INTERFACE COMMANDS

These commands are used to display or set communication parameters for an Ethernet port, aggregated link, or VLAN; or perform cable diagnostics on the specified interface.

**Table 1: Interface Commands**

| Command | Function | Mode |
|---|---|---|
| *Interface Configuration* | | |
| interface | Configures an interface type and enters interface configuration mode | GC |
| alias | Configures an alias name for the interface | IC |
| capabilities | Advertises the capabilities of a given interface for use in autonegotiation | IC |
| description | Adds a description to an interface configuration | IC |
| flowcontrol | Enables flow control on a given interface | IC |
| media-type | Force port type selected for combination ports | IC |
| negotiation | Enables autonegotiation of a given interface | IC |
| shutdown | Disables an interface | IC |
| speed-duplex | Configures the speed and duplex operation of a given interface when autonegotiation is disabled | IC |
| switchport packet-rate | Configures broadcast, multicast and unknown unicast storm control thresholds | IC |
| clear counters | Clears statistics on an interface | PE |
| show interfaces counters | Displays statistics for the specified interfaces | NE, PE |
| show interfaces status | Displays status for the specified interface | NE, PE |
| show interfaces switchport | Displays the administrative and operational status of an interface | NE, PE |
| show interfaces transceiver | Displays the temperature, voltage, bias current, transmit power, and receive power | PE |
| *Cable Diagnostics* | | |
| test cable-diagnostics dsp | Performs cable diagnostics on the specified port | PE |
| test loop internal | Performs internal loop back test on the specified port | PE |
| show cable-diagnostics dsp | Shows the results of a cable diagnostics test | PE |
| show loop internal | Shows the results of a loop back test | PE |

**interface** This command configures an interface type and enters interface configuration mode. Use the **no** form with a trunk to remove an inactive interface. Use the **no** form with a Layer 3 VLAN (normal type) to change it back to a Layer 2 interface.

### SYNTAX

[**no**] **interface** *interface*

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

**vlan** *vlan-id* (Range: 1-4093)

### DEFAULT SETTING

None

### COMMAND MODE

Global Configuration

### EXAMPLE

To specify port 4, enter the following command:

```
Console(config)#interface ethernet 1/4
Console(config-if)#
```

**alias** This command configures an alias name for the interface. Use the **no** form to remove the alias name.

### SYNTAX

**alias** *string*

**no alias**

*string* - A mnemonic name to help you remember what is attached to this interface. (Range: 1-64 characters)

### DEFAULT SETTING

None

### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE

The alias is displayed in the running-configuration file. An example of the value which a network manager might store in this object for a WAN interface is the (Telco's) circuit number/identifier of the interface.

#### EXAMPLE

The following example adds an alias to port 4.

```
Console(config)#interface ethernet 1/4
Console(config-if)#alias finance
Console(config-if)#
```

## capabilities

This command advertises the port capabilities of a given interface during auto-negotiation. Use the **no** form with parameters to remove an advertised capability, or the **no** form without parameters to restore the default values.

#### SYNTAX

[**no**] **capabilities** {**10000full** | **1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**}

**10000full** - Supports 10 Gbps full-duplex operation

**1000full** - Supports 1 Gbps full-duplex operation

**100full** - Supports 100 Mbps full-duplex operation

**100half** - Supports 100 Mbps half-duplex operation

**10full** - Supports 10 Mbps full-duplex operation

**10half** - Supports 10 Mbps half-duplex operation

**flowcontrol** - Supports flow control

**symmetric** (Gigabit and 10 Gigabit only) - When specified, the port transmits and receives symmetric pause frames.

#### DEFAULT SETTING

1000BASE-T: 10half, 10full, 100half, 100full, 1000full
1000BASE-SX/LX/LH (SFP): 1000full
10GBASE-SR/LR/ER (XFP): 10Gfull
10GBASE-T: 10Gfull

#### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

#### COMMAND USAGE

- 10GBASE-XFP connections are fixed at 10G, full duplex. When auto-negotiation is enabled, the only attributes which can be advertised include flow control and symmetric pause frames.

- The 1000BASE-T and 10GBASE-T standard does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T and 10GBASE-T port or trunk.

- When auto-negotiation is enabled with the negotiation command, the switch will negotiate the best settings for a link based on the **capabilities** command. When auto-negotiation is disabled, you must manually specify the link attributes with the speed-duplex and flowcontrol commands.

#### EXAMPLE

The following example configures Ethernet port 5 capabilities to include 100half and 100full.

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

#### RELATED COMMANDS

negotiation (810)
speed-duplex (812)
flowcontrol (808)

### description

This command adds a description to an interface. Use the **no** form to remove the description.

#### SYNTAX

**description** *string*

**no description**

*string* - Comment or a description to help you remember what is attached to this interface. (Range: 1-64 characters)

#### DEFAULT SETTING

None

#### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

#### COMMAND USAGE

The description is displayed by the show interfaces status command and in the running-configuration file. An example of the value which a network manager might store in this object is the name of the manufacturer, and the product name.

#### EXAMPLE

The following example adds a description to port 4.

```
Console(config)#interface ethernet 1/4
Console(config-if)#description RD-SW#3
Console(config-if)#
```

### flowcontrol

This command enables flow control. Use the **no** form to disable flow control.

### SYNTAX

[**no**] **flowcontrol**

### DEFAULT SETTING
Disabled

### COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE
- 1000BASE-T and 10GBASE-T do not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T and 10GBASE-T port or trunk.

- Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3-2002 (formally IEEE 802.3x) for full-duplex operation.

- To force flow control on or off (with the **flowcontrol** or **no flowcontrol** command), use the **no negotiation** command to disable auto-negotiation on the selected interface.

- When using the negotiation command to enable auto-negotiation, the optimal settings will be determined by the capabilities command. To enable flow control under auto-negotiation, “flowcontrol” must be included in the capabilities list for any port

- Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.

### EXAMPLE
The following example enables flow control on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

### RELATED COMMANDS
negotiation (810)
capabilities (flowcontrol, symmetric) (807)

## media-type

This command forces the port type selected for combination ports 25-26. Use the **no** form to restore the default mode.

### SYNTAX

**media-type** *mode*

**no media-type**

*mode*

**copper-forced** - Always uses the built-in RJ-45 port.

**sfp-forced** - Always uses the SFP port (even if a module not installed).

**sfp-preferred-auto** - Uses SFP port if both combination types are functioning and the SFP port has a valid link.

### DEFAULT SETTING

Ports 1-20/1-44: copper-forced
Ports 21-24/45-48: sfp-preferred-auto
Ports 25-26/49-50: sfp-preferred-auto

### COMMAND MODE

Interface Configuration (Ethernet)

### EXAMPLE

This forces the switch to use the built-in RJ-45 port for the combination port 25.

```
Console(config)#interface ethernet 1/25
Console(config-if)#media-type copper-forced
Console(config-if)#
```

## negotiation

This command enables auto-negotiation for a given interface. Use the **no** form to disable auto-negotiation.

### SYNTAX

[**no**] **negotiation**

### DEFAULT SETTING

Enabled

### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE

- 1000BASE-T and 10GBASE-T do not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T and 10GBASE-T port or trunk.

- When auto-negotiation is enabled the switch will negotiate the best settings for a link based on the capabilities command. When auto-negotiation is disabled, you must manually specify the link attributes with the speed-duplex and flowcontrol commands.

- If auto-negotiation is disabled, auto-MDI/MDI-X pin signal configuration will also be disabled for the RJ-45 ports.

#### EXAMPLE

The following example configures port 11 to use auto-negotiation.

```
Console(config)#interface ethernet 1/11
Console(config-if)#negotiation
Console(config-if)#
```

#### RELATED COMMANDS

capabilities (807)
speed-duplex (812)

### shutdown

This command disables an interface. To restart a disabled interface, use the **no** form.

#### SYNTAX

[**no**] **shutdown**

#### DEFAULT SETTING

All interfaces are enabled.

#### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

#### COMMAND USAGE

This command allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also want to disable a port for security reasons.

#### EXAMPLE

The following example disables port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#shutdown
Console(config-if)#
```

## speed-duplex

This command configures the speed and duplex mode of a given interface when auto-negotiation is disabled. Use the **no** form to restore the default.

### SYNTAX

**speed-duplex** {**1000full** | **100full** | **100half** | **10full** | **10half**}

**no speed-duplex**

**1000full** - Forces 1 Gbps 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 on the Gigabit ports, and disabled on the 10 Gigabit ports.
- When auto-negotiation is disabled, the default speed-duplex setting is 100full on the 1000Base-T ports, 1000full on the 1000Base SFP ports, and 10Gfull on the 10G ports.
- The speed-duplex setting on the 10G ports is fixed at 10Gfull.

### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE

- The 1000BASE-T and 10GBASE-T standard does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T and 10GBASE-T port or trunk. If not used, the success of the link process cannot be guaranteed when connecting to other types of switches.
- To force operation to the speed and duplex mode specified in a **speed-duplex** command, use the no negotiation command to disable auto-negotiation on the selected interface.
- When using the negotiation command to enable auto-negotiation, the optimal settings will be determined by the capabilities command. To set the speed/duplex mode under auto-negotiation, the required mode must be specified in the capabilities list for an interface.

### EXAMPLE

The following example configures port 5 to 100 Mbps, half-duplex operation.

```
Console(config)#interface ethernet 1/5
Console(config-if)#speed-duplex 100half
Console(config-if)#no negotiation
Console(config-if)#
```

**RELATED COMMANDS**

negotiation (810)
capabilities (807)

## switchport packet-rate

This command configures broadcast, multicast and unknown unicast storm control. Use the **no** form to restore the default setting.

**SYNTAX**

**switchport** {**broadcast** | **multicast** | **unicast**} **packet-rate** *rate*

**no switchport** {**broadcast** | **multicast** | **unicast**}

*rate* - Threshold level as a rate; i.e., packets per second. (Range: 500-262143)

**DEFAULT SETTING**

Broadcast Storm Control: Enabled, packet-rate limit: 500 pps
Multicast Storm Control: Disabled
Unknown Unicast Storm Control: Disabled

**COMMAND MODE**

Interface Configuration (Ethernet)

**COMMAND USAGE**

- When traffic exceeds the threshold specified for broadcast and multicast or unknown unicast traffic, packets exceeding the threshold are dropped until the rate falls back down beneath the threshold.

- Traffic storms can be controlled at the hardware level using this command or at the software level using the auto-traffic-control command. However, only one of these control types can be applied to a port. Enabling hardware-level storm control on a port will disable automatic storm control on that port.

- The rate limits set by this command are also used by automatic storm control when the control response is set to rate limiting by the auto-traffic-control action command.

- Using both rate limiting and storm control on the same interface may lead to unexpected results. For example, suppose broadcast storm control is set to 500 pps by the command “switchport broadcast packet-rate 500" and the rate limit is set to 200 Mbps by the command “rate-limit input 20" on a port. Since 200 Mbps is 1/5 of line speed (1000 Mbps), the received rate will actually be 100 pps, or 1/5 of the 500 pps limit set by the storm control command. It is therefore not advisable to use both of these commands on the same interface.

#### EXAMPLE

The following shows how to configure broadcast storm control at 600 packets per second:

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast packet-rate 600
Console(config-if)#
```

## clear counters

This command clears statistics on an interface.

#### SYNTAX

**clear counters** *interface*

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-26)

**port-channel** *channel-id* (Range: 1-32)

#### 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 counters

This command displays interface statistics.

### SYNTAX

**show interfaces counters** [*interface*]

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-26)

**port-channel** *channel-id* (Range: 1-32)

### DEFAULT SETTING

Shows the counters for all interfaces.

### COMMAND MODE

Normal Exec, Privileged Exec

### COMMAND USAGE

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see "Showing Port or Trunk Statistics" on page 113.

### EXAMPLE

```
Console#show interfaces counters ethernet 1/17
Ethernet 1/ 1
 ===== IF table Stats =====
                138550 Octets Input
                820500 Octets Output
                   734 Unicast Input
                   932 Unicast Output
                    12 Discard Input
                     0 Discard Output
                     0 Error Input
                     0 Error Output
                     0 Unknown Protos Input
                     0 QLen Output
 ===== Extended Iftable Stats =====
                    38 Multi-cast Input
                  1342 Multi-cast Output
                   210 Broadcast Input
                     2 Broadcast Output
 ===== Ether-like Stats =====
                     0 Alignment Errors
                     0 FCS Errors
                     0 Single Collision Frames
                     0 Multiple Collision Frames
                     0 SQE Test Errors
                     0 Deferred Transmissions
                     0 Late Collisions
                     0 Excessive Collisions
                     0 Internal Mac Transmit Errors
                     0 Internal Mac Receive Errors
                     0 Frames Too Long
                     0 Carrier Sense Errors
                     0 Symbol Errors
 ===== RMON Stats =====
                     0 Drop Events
```

```
           959114 Octets
             3259 Packets
              212 Broadcast PKTS
             1381 Multi-cast PKTS
                0 Undersize PKTS
                0 Oversize PKTS
                0 Fragments
                0 Jabbers
                0 CRC Align Errors
                0 Collisions
             2142 Packet Size <= 64 Octets
              303 Packet Size 65 to 127 Octets
              140 Packet Size 128 to 255 Octets
               75 Packet Size 256 to 511 Octets
              140 Packet Size 512 to 1023 Octets
              459 Packet Size 1024 to 1518 Octets
 ===== Port Utilization =====
               35 Octets Input per seconds
                0 Packets Input per seconds
             0.00 % Input Utilization
               56 Octets Output per seconds
                0 Packets Output per second
             0.00 % Output Utilization
Console#
```

## show interfaces status

This command displays the status for an interface.

### SYNTAX

**show interfaces status** [*interface*]

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-26)

**port-channel** *channel-id* (Range: 1-32)

**vlan** *vlan-id* (Range: 1-4093)

### DEFAULT SETTING

Shows the status for all interfaces.

### COMMAND MODE

Normal Exec, Privileged Exec

### COMMAND USAGE

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see "Displaying Connection Status" on page 110.

### EXAMPLE

```
Console#show interfaces status ethernet 1/21
 Basic Information:
  Port Type           : 1000T
  Mac Address         : 00-00-E8-93-82-A1
 Configuration:
```

```
Name                 :
Port Admin           : Up
Speed-duplex         : Auto
Capabilities         : 10half, 10full, 100half, 100full, 1000full
Broadcast Storm      : Enabled
Broadcast Storm Limit  : 500 packets/second
Flow Control         : Disabled
VLAN Trunking        : Disabled
LACP                 : Disabled
Mac-Learning         : Yes
Port Security        : Disabled
Max MAC Count        : 0
Port Security Action  : None
Media Type           : Copper forced
MTU                  : 1518
Current Status:
Link Status          : Up
Port Operation Status  : Up
Operation Speed-duplex : 100full
Flow Control Type    : None
Console#
```

## show interfaces switchport

This command displays the administrative and operational status of the specified interfaces.

### SYNTAX

**show interfaces switchport** [*interface*]

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-26)

**port-channel** *channel-id* (Range: 1-32)

### DEFAULT SETTING

Shows all interfaces.

### COMMAND MODE

Normal Exec, Privileged Exec

### COMMAND USAGE

If no interface is specified, information on all interfaces is displayed.

### EXAMPLE

This example shows the configuration setting for port 21.

```
Console#show interfaces switchport ethernet 1/21
Information of Eth 1/1
 Broadcast Threshold       : Enabled, 500 packets/second
 LACP Status               : Disabled
 Ingress Rate Limit        : Disabled, 1000M bits per second
 Egress Rate Limit         : Disabled, 1000M bits per second
 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
  802.1Q-tunnel Status:         Disable
  802.1Q-tunnel Mode:            NORMAL
  802.1Q-tunnel TPID:           8100(Hex)
Console#
```

**Table 2: show interfaces switchport** - display description

| Field | Description |
|---|---|
| Broadcast Threshold | Shows if broadcast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 813). |
| LACP Status | Shows if Link Aggregation Control Protocol has been enabled or disabled (page 825). |
| Ingress/Egress Rate Limit | Shows if rate limiting is enabled, and the current rate limit (page 837). |
| VLAN Membership Mode | Indicates membership mode as Trunk or Hybrid (page 896). |
| Ingress Rule | Shows if ingress filtering is enabled or disabled (page 895). |
| Acceptable Frame Type | Shows if acceptable VLAN frames include all types or tagged frames only (page 893). |
| Native VLAN | Indicates the default Port VLAN ID (page 896). |
| Priority for Untagged Traffic | Indicates the default priority for untagged frames (page 931). |
| GVRP Status | Shows if GARP VLAN Registration Protocol is enabled or disabled (page 888). |
| Allowed VLAN | Shows the VLANs this interface has joined, where “(u)” indicates untagged and “(t)” indicates tagged (page 894). |
| Forbidden VLAN | Shows the VLANs this interface can not dynamically join via GVRP (page 888). |
| Private-VLAN Mode | Shows the private VLAN mode as host, promiscuous, or none (909). |
| Private VLAN host-association | Shows the secondary (or community) VLAN with which this port is associated (910). |
| Private VLAN mapping | Shows the primary VLAN mapping for a promiscuous port (910). |
| 802.1Q-tunnel Status | Shows if 802.1Q tunnel is enabled on this interface (901). |
| 802.1Q-tunnel Mode | Shows the tunnel mode as Normal, 802.1Q Tunnel or 802.1Q Tunnel Uplink (901). |
| 802.1Q-tunnel TPID | Shows the Tag Protocol Identifier used for learning and switching packets (903). |

## show interfaces transceiver

This command displays identifying information for the specified transceiver, as well as the temperature, voltage, bias current, transmit power, and receive power.

### SYNTAX

**show interfaces transceiver** [*interface*]

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 21-24)

### DEFAULT SETTING

Shows all SFP interfaces.

### COMMAND MODE

Privileged Exec

### COMMAND USAGE

The switch can display diagnostic information for SFP modules which support the SFF-8472 Specification for Diagnostic Monitoring Interface for Optical Transceivers. This information allows administrators to remotely diagnose problems with optical devices.

### EXAMPLE

```
Console#show interfaces transceiver ethernet 1/24
Information of Eth 1/24
 Connector Type        : LC
 Fiber Type            : Single Mode (SM)
 Eth Compliance Codes  : 1000BASE-LX
 Tx Central Wavelength : 1310 nm
 Baud Rate             : 1300 MBd
 Vendor OUI            : 00-00-00
 Vendor Name           : DELTA
 Vendor PN             : LCP-1250B4QDRT
 Vendor Rev            : 000
 Vendor SN             : 0000070904100004
 Date Code             : 07-03-02
 Temperature           : 56 degrees C
 Vcc                   : 3.33 V
 Bias Current          : 25.34 mA
 TX Power              : 270 uW
 RX Power              : 0 uW
Console#sh interfaces transceiver e 1/26
Information of Eth 1/26
 Connector Type        : LC
 Fiber Type            : [0x00]
 10G Eth Compliance    : 10GBASE-LR, 10GBASE-LW
 Tx Central Wavelength : 26150 nm
 Baud Rate             : 9900 MBd
 Vendor OUI            : 00-09-A6
 Vendor Name           : BOOKHAM-TECHNOL-
 Vendor PN             : IGF17311
 Vendor Rev            : B2
 Vendor SN             :
 Date Code             : 240-240-240
 Temperature           : 44 degrees C
 Vcc                   : 0.00 V
 Bias Current          : 43.11 mA
```

```
 TX Power          : 605 uW
 RX Power          : 3 uW
Console#
```

## test cable-diagnostics dsp

This command performs cable diagnostics on the specified port to diagnose any cable faults (short, open, etc.) and report the cable length.

### SYNTAX

**test cable-diagnostics dsp interface** *interface*

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-24)

### COMMAND MODE

Privileged Exec

### COMMAND USAGE

- Cable diagnostics are performed using Digital Signal Processing (DSP) test methods.
- This cable test is only accurate for cables 7 - 140 meters long.
- The test takes approximately 5 seconds. The switch displays the results of the test immediately upon completion, including common cable failures, as well as the status and approximate length of each cable pair.
- Potential conditions which may be listed by the diagnostics include:
  - OK: Correctly terminated pair
  - Open: Open pair, no link partner
  - Short: Shorted pair
  - Not Supported: This message is displayed for any Gigabit Ethernet ports linked up at a speed lower than 1000 Mbps, or for any 10G Ethernet ports.
  - Impedance mismatch: Terminating impedance is not in the reference range.
- Ports are linked down while running cable diagnostics.

### EXAMPLE

```
Console#test cable-diagnostics dsp interface ethernet 1/1
Cable Diagnostics on interface Ethernet 1/1:
 Cable Short with accuracy 0 meters.
   Pair A OK, length 1 meters
   Pair B OK, length 2 meters
   Pair C Short, length 1 meters
   Pair D Short, length 2 meters
   Last Update 0n 2010-04-23 07:59:26

  Console#
```

## test loop internal

This command performs an internal loop back test on the specified port.

### SYNTAX

**test loop internal interface** *interface*

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

### COMMAND MODE

Privileged Exec

### COMMAND USAGE

When performing an internal loopback test, packets from the specified interface are looped back into its internal PHY. Outgoing data is looped back to the receiver without actually being transmitted. Internal loopback makes it possible to check that an interface is working properly without having to make any network connections.

### EXAMPLE

```
Console#test loop internal interface ethernet 1/1
Internal loopback test: succeeded
Console#
```

## show cable-diagnostics dsp

This command shows the results of a cable diagnostics test.

### SYNTAX

**show cable-diagnostics dsp interface** [*interface*]

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-24)

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show cable-diagnostics dsp interface ethernet 1/1
Cable Diagnostics on interface Ethernet 1/1:
 Cable OK with accuracy 0 meters.
   Pair A OK, length 0 meters
   Pair B OK, length 0 meters
   Pair C OK, length 1 meters
   Pair D OK, length 1 meters
   Last Update 0n 2009-10-21 15:08:20

Console#
```

## show loop internal

This command shows the results of a loop back test.

### SYNTAX

**show loop internal interface** [*interface*]

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show loop internal interface ethernet 1/1

 Port     Test Result    Last Update
 -------- -------------- --------------------
 Eth 1/1       Succeeded  2024-07-15 15:26:56
Console#
```

# 33 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. The MIL300 series switches support up to 9 trunks depending on the model. For example, a trunk consisting of two 1000 Mbps ports can support an aggregate bandwidth of 4 Gbps when operating at full duplex.

**Table 1: Link Aggregation Commands**

| Command | Function | Mode |
|---|---|---|
| *Manual Configuration Commands* | | |
| interface port-channel | Configures a trunk and enters interface configuration mode for the trunk | GC |
| channel-group | Adds a port to a trunk | IC (Ethernet) |
| *Dynamic Configuration Commands* | | |
| lacp | Configures LACP for the current interface | IC (Ethernet) |
| lacp admin-key | Configures a port's administration key | IC (Ethernet) |
| lacp port-priority | Configures a port's LACP port priority | IC (Ethernet) |
| lacp system-priority | Configures a port's LACP system priority | IC (Ethernet) |
| lacp admin-key | Configures an port channel's administration key | IC (Port Channel) |
| *Trunk Status Display Commands* | | |
| show interfaces status port-channel | Shows trunk information | NE, PE |
| show lacp | Shows LACP information | PE |

## GUIDELINES FOR CREATING TRUNKS

*General Guidelines –*

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- A trunk can have up to 8 ports.
- The ports at both ends of a connection must be configured as trunk ports.
- All ports in a trunk must be configured in an identical manner, including communication mode (i.e., speed and duplex mode), VLAN assignments, and CoS settings.
- Any of the Gigabit ports on the front panel can be trunked together, including ports of different media types.

- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN via the specified port-channel.
- STP, VLAN, and IGMP settings can only be made for the entire trunk via the specified port-channel.

*Dynamically Creating a Port Channel* –

Ports assigned to a common port channel must meet the following criteria:

- Ports must have the same LACP system priority.
- Ports must have the same port admin key (Ethernet Interface).
- If the port channel admin key (lacp admin key - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (lacp admin key - Ethernet Interface) used by the interfaces that joined the group.
- However, if the port channel admin key is set, then the port admin key must be set to the same value for a port to be allowed to join a channel group.
- If a link goes down, LACP port priority is used to select the backup link.

## channel-group

This command adds a port to a trunk. Use the **no** form to remove a port from a trunk.

### SYNTAX

**channel-group** *channel-id*

**no channel-group**

*channel-id* - Trunk index (Range: 1-32)

### DEFAULT SETTING

The current port will be added to this trunk.

### COMMAND MODE

Interface Configuration (Ethernet)

### COMMAND USAGE

- When configuring static trunks, the switches must comply with the Cisco EtherChannel standard.
- Use **no channel-group** to remove a port group from a trunk.
- Use no interface port-channel to remove a trunk from the switch.

### EXAMPLE

The following example creates trunk 1 and then adds port 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)#
```

## lacp

This command enables 802.3ad Link Aggregation Control Protocol (LACP) for the current interface. Use the **no** form to disable it.

### SYNTAX

[**no**] **lacp**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Interface Configuration (Ethernet)

### COMMAND USAGE

- The ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.
- A trunk formed with another switch using LACP will automatically be assigned the next available port-channel ID.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.

### EXAMPLE

The following shows LACP enabled on ports 10-12. Because LACP has also been enabled on the ports at the other end of the links, the show interfaces status port-channel 1 command shows that Trunk1 has been established.

```
Console(config)#interface ethernet 1/10
Console(config-if)#lacp
Console(config-if)#interface ethernet 1/11
Console(config-if)#lacp
Console(config-if)#interface ethernet 1/12
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 1
Information of Trunk 1
 Basic Information:
  Port Type              : 1000T
  Mac Address            : 12-34-12-34-12-3F
Configuration:
  Name                   :
  Port Admin             : Up
  Speed-duplex           : Auto
  Capabilities           : 10half, 10full, 100half, 100full, 1000full
  Flow Control           : 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          : Eth1/10, Eth1/11, Eth1/12,
Console#
```

## lacp admin-key (Ethernet Interface)

This command configures a port's LACP administration key. Use the **no** form to restore the default setting.

### SYNTAX

**lacp** {**actor** | **partner**} **admin-key** *key*

**no lacp** {**actor** | **partner**} **admin-key**

**actor** - The local side an aggregate link.

**partner** - The remote side of an aggregate link.

*key* - The port admin key must be set to the same value for ports that belong to the same link aggregation group (LAG). (Range: 0-65535)

### DEFAULT SETTING

0

### COMMAND MODE

Interface Configuration (Ethernet)

### COMMAND USAGE

- Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).
- If the port channel admin key (lacp admin key - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (**lacp admin key** - Ethernet Interface) used by the interfaces that joined the group.
- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state.

### EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor admin-key 120
Console(config-if)#
```

## lacp port-priority

This command configures LACP port priority. Use the **no** form to restore the default setting.

### SYNTAX

**lacp** {**actor** | **partner**} **port-priority** *priority*

**no lacp** {**actor** | **partner**} **port-priority**

**actor** - The local side an aggregate link.

**partner** - The remote side of an aggregate link.

*priority* - LACP port priority is used to select a backup link. (Range: 0-65535)

### DEFAULT SETTING

32768

### COMMAND MODE

Interface Configuration (Ethernet)

### COMMAND USAGE

- Setting a lower value indicates a higher effective priority.
- If an active port link goes down, the backup port with the highest priority is selected to replace the downed link. However, if two or more ports have the same LACP port priority, the port with the lowest physical port number will be selected as the backup port.
- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

### EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor port-priority 128
```

## lacp system-priority

This command configures a port's LACP system priority. Use the **no** form to restore the default setting.

### SYNTAX

**lacp** {**actor** | **partner**} **system-priority** *priority*

**no lacp** {**actor** | **partner**} **system-priority**

**actor** - The local side an aggregate link.

**partner** - The remote side of an aggregate link.

*priority* - This priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535)

**DEFAULT SETTING**
32768

**COMMAND MODE**
Interface Configuration (Ethernet)

**COMMAND USAGE**
- Port must be configured with the same system priority to join the same LAG.
- System priority is combined with the switch's MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.
- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

**EXAMPLE**

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor system-priority 3
Console(config-if)#
```

## lacp admin-key (Port Channel)

This command configures a port channel's LACP administration key string. Use the **no** form to restore the default setting.

**SYNTAX**

**lacp admin-key** *key*

**no lacp admin-key**

*key* - The port channel admin key is used to identify a specific link aggregation group (LAG) during local LACP setup on this switch. (Range: 0-65535)

**DEFAULT SETTING**
0

**COMMAND MODE**
Interface Configuration (Port Channel)

**COMMAND USAGE**
- Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).
- If the port channel admin key (**lacp admin key** - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (lacp admin key - Ethernet Interface) used by the interfaces that joined the group. Note that when the LAG is no longer used, the port channel admin key is reset to 0.

**EXAMPLE**

```
Console(config)#interface port-channel 1
Console(config-if)#lacp admin-key 3
Console(config-if)#
```

## show lacp

This command displays LACP information.

### SYNTAX

**show lacp** [*port-channel*] {**counters** | **internal** | **neighbors** | **sys-id**}

*port-channel* - Local identifier for a link aggregation group. (Range: 1-32)

**counters** - Statistics for LACP protocol messages.

**internal** - Configuration settings and operational state for local side.

**neighbors** - Configuration settings and operational state for remote side.

**sys-id** - Summary of system priority and MAC address for all channel groups.

### DEFAULT SETTING

Port Channel: all

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show lacp 1 counters
Port Channel: 1
-------------------------------------------------------------------------
Eth 1/ 2
-------------------------------------------------------------------------
 LACPDUs Sent        : 12
 LACPDUs Received    : 6
 Marker Sent         : 0
 Marker Received     : 0
 LACPDUs Unknown Pkts : 0
 LACPDUs Illegal Pkts : 0
:
```

**Table 2: show lacp counters** - display description

| Field | Description |
|---|---|
| LACPDUs Sent | Number of valid LACPDUs transmitted from this channel group. |
| LACPDUs Received | Number of valid LACPDUs received on this channel group. |
| Marker Sent | Number of valid Marker PDUs transmitted from this channel group. |
| Marker Received | Number of valid Marker PDUs received by this channel group. |
| LACPDUs Unknown Pkts | Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type. |
| LACPDUs Illegal Pkts | Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype. |

```
Console#show lacp 1 internal
Port Channel : 1
-------------------------------------------------------------------------
Oper Key  : 3
Admin Key : 0
Eth 1/ 1
-------------------------------------------------------------------------
 LACPDUs Internal     : 30 seconds
 LACP System Priority : 32768
 LACP Port Priority   : 32768
 Admin Key            : 3
 Oper Key             : 3
 Admin State          : defaulted, aggregation, long timeout, LACP-activity
 Oper State           : distributing, collecting, synchronization,
                        aggregation, long timeout, LACP-activity
:
```

**Table 3: show lacp internal** - display description

| Field | Description |
|---|---|
| Oper Key | Current operational value of the key for the aggregation port. |
| Admin Key | Current administrative value of the key for the aggregation port. |
| LACPDUs Internal | Number of seconds before invalidating received LACPDU information. |
| LACP System Priority | LACP system priority assigned to this port channel. |
| 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:<br>◆Expired – The actor's receive machine is in the expired state;<br>◆Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner.<br>◆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.<br>◆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.<br>◆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.<br>◆Aggregation – The system considers this link to be aggregatable; i.e., a potential candidate for aggregation.<br>◆Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate.<br>◆LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active) |

```
Console#show lacp 1 neighbors
Port Channel 1 neighbors
-------------------------------------------------------------------------
Eth 1/ 1
-------------------------------------------------------------------------
 Partner Admin System ID   : 32768, 00-00-00-00-00-00
 Partner Oper System ID    : 32768, 00-12-CF-61-24-2F
 Partner Admin Port Number : 1
 Partner Oper Port Number  : 1
```

```
Port Admin Priority      : 32768
Port Oper Priority       : 32768
Admin Key                : 0
Oper Key                 : 3
Admin State:               defaulted, distributing, collecting,
                         synchronization, long timeout,
Oper State:                distributing, collecting, synchronization,
                         aggregation, long timeout, LACP-activity
:
```

**Table 4: show lacp neighbors** - display description

| Field | Description |
|---|---|
| Partner Admin System ID | LAG partner's system ID assigned by the user. |
| Partner Oper System ID | LAG partner's system ID assigned by the LACP protocol. |
| Partner Admin Port Number | Current administrative value of the port number for the protocol Partner. |
| Partner Oper Port Number | Operational port number assigned to this aggregation port by the port's protocol partner. |
| Port Admin Priority | Current administrative value of the port priority for the protocol partner. |
| Port Oper Priority | Priority value assigned to this aggregation port by the partner. |
| Admin Key | Current administrative value of the Key for the protocol partner. |
| Oper Key | Current operational value of the Key for the protocol partner. |
| Admin State | Administrative values of the partner's state parameters. (See preceding table.) |
| Oper State | Operational values of the partner's state parameters. (See preceding table.) |

```
Console#show lacp sysid
Port Channel    System Priority    System MAC Address
-------------------------------------------------------------------------
      1           32768     00-30-F1-8F-2C-A7
      2           32768     00-30-F1-8F-2C-A7
      3           32768     00-30-F1-8F-2C-A7
      4           32768     00-30-F1-8F-2C-A7
      5           32768     00-30-F1-8F-2C-A7
      6           32768     00-30-F1-8F-2C-A7
      7           32768     00-30-F1-D4-73-A0
      8           32768     00-30-F1-D4-73-A0
      9           32768     00-30-F1-D4-73-A0
     10           32768     00-30-F1-D4-73-A0
     11           32768     00-30-F1-D4-73-A0
     12           32768     00-30-F1-D4-73-A0
:
```

**Table 5: show lacp sysid** - display description

| Field | Description |
|---|---|
| Channel group | A link aggregation group configured on this switch. |
| System Priority[1] | LACP system priority for this channel group. |
| System MAC Address* | System MAC address. |

1. The LACP system priority and system MAC address are concatenated to form the LAG system ID.

# 34 PORT MIRRORING COMMANDS

Data can be mirrored from a local port on the same switch or from a remote port on another switch for analysis at the target port using software monitoring tools or a hardware probe. This switch supports the following mirroring modes.

**Table 1: Port Mirroring Commands**

| Command | Function |
|---|---|
| Local Port Mirroring | Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port |

## LOCAL PORT MIRRORING COMMANDS

This section describes how to mirror traffic from a source port to a target port.

**Table 2: Mirror Port Commands**

| Command | Function | Mode |
|---|---|---|
| port monitor | Configures a mirror session | IC |
| show port monitor | Shows the configuration for a mirror port | PE |

### port monitor

This command configures a mirror session. Use the **no** form to clear a mirror session.

#### SYNTAX

**port monitor** {*interface* [**rx** | **tx** | **both**]}

**no port monitor** *interface*

*interface* - **ethernet** *unit*/*port* (source port)

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**rx** - Mirror received packets.

**tx** - Mirror transmitted packets.

**both** - Mirror both received and transmitted packets.

#### DEFAULT SETTING

- No mirror session is defined.
- When enabled for an interface, default mirroring is for both received and transmitted packets.

#### COMMAND MODE
Interface Configuration (Ethernet, destination port)

#### COMMAND USAGE
- You can mirror traffic from any source port to a destination port for real-time analysis. You can then attach a logic analyzer or RMON probe to the destination port and study the traffic crossing the source port in a completely unobtrusive manner.
- Set the destination port by specifying an Ethernet interface with the interface configuration command, and then use the **port monitor** command to specify the source of the traffic to mirror.
- When mirroring traffic from a port, the mirror port and monitor port speeds should match, otherwise traffic may be dropped from the monitor port.
- You can create multiple mirror sessions, but all sessions must share the same destination port.
- Spanning Tree BPDU packets are not mirrored to the target port.

#### EXAMPLE
The following example configures the switch to mirror all packets from port 6 to 11:

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6 both
Console(config-if)#
```

## show port monitor

This command displays mirror information.

#### SYNTAX

**show port monitor** [*interface*]

*interface* - **ethernet** *unit*/*port* (source port)

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

#### DEFAULT SETTING
Shows all sessions.

#### COMMAND MODE
Privileged Exec

#### COMMAND USAGE
This command displays the currently configured source port, destination port, and mirror mode (i.e., RX, TX, RX/TX).

#### 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
Console(config-if)#end
Console#show port monitor
Port Mirroring
-------------------------------------
 Destination Port (listen port): Eth1/1
 Source Port (monitored port):   Eth1/6
 Mode                          :RX/TX
Console#
```

# 35 RATE LIMIT COMMANDS

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

Rate limiting can be applied to individual ports 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.

**Table 1: Rate Limit Commands**

| Command | Function | Mode |
|---|---|---|
| rate-limit | Configures the maximum input or output rate for an interface | IC |

## rate-limit

This command defines the rate limit for a specific interface. Use this command without specifying a rate to restore the default rate. Use the **no** form to restore the default status of disabled.

### SYNTAX

**rate-limit** {**input** | **output**} [*rate*]

**no rate-limit** {**input** | **output**}

**input** – Input rate for specified interface

**output** – Output rate for specified interface

*rate* – Maximum value in Mbps.
(Range: 64-1000000 kbps for Gigabit Ethernet ports
64-10000000 kbps for 10 Gigabit Ethernet ports)

### DEFAULT SETTING

1000 Mbps

### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE

Using both rate limiting and storm control on the same interface may lead to unexpected results. For example, suppose broadcast storm control is set to 500 pps by the command “switchport broadcast packet-rate 500,” and the rate limit is set to 20 Mbps by the command “rate-limit input 20" on a port. Since 20 Mbps is 1/5 of line speed (100 Mbps), the received rate will actually be 100 pps, or 1/5 of the 500 pps limit set by the storm control command. It is therefore not advisable to use both of these commands on the same interface.

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input 64
Console(config-if)#
```

### RELATED COMMAND

show interfaces switchport (817)

# 36 AUTOMATIC TRAFFIC CONTROL COMMANDS

Automatic Traffic Control (ATC) configures bounding thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port.

**Table 1: ATC Commands**

| Command | Function | Mode |
|---|---|---|
| *Threshold Commands* | | |
| auto-traffic-control apply-timer | Sets the time at which to apply the control response after ingress traffic has exceeded the upper threshold | GC |
| auto-traffic-control release-timer | Sets the time at which to release the control response after ingress traffic has fallen beneath the lower threshold | GC |
| auto-traffic-control[1] | Enables automatic traffic control for broadcast or multicast storms | IC (Port) |
| auto-traffic-control action | Sets the control action to limit ingress traffic or shut down the offending port | IC (Port) |
| auto-traffic-control alarm-clear-threshold | Sets the lower threshold for ingress traffic beneath which a cleared storm control trap is sent | IC (Port) |
| auto-traffic-control alarm-fire-threshold | Sets the upper threshold for ingress traffic beyond which a storm control response is triggered after the apply timer expires | IC (Port) |
| auto-traffic-control auto-control-release | Automatically releases a control response | IC (Port) |
| auto-traffic-control control-release | Manually releases a control response | PE |
| *SNMP Trap Commands* | | |
| snmp-server enable port-traps atc broadcast-alarm-clear | Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered | IC (Port) |
| snmp-server enable port-traps atc broadcast-alarm-fire | Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control | IC (Port) |
| snmp-server enable port-traps atc broadcast-control-apply | Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control and the apply timer expires | IC (Port) |
| snmp-server enable port-traps atc broadcast-control-release | Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires | IC (Port) |
| snmp-server enable port-traps atc multicast-alarm-clear | Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered | IC (Port) |
| snmp-server enable port-traps atc multicast-alarm-fire | Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control | IC (Port) |

**Table 1: ATC Commands (Continued)**

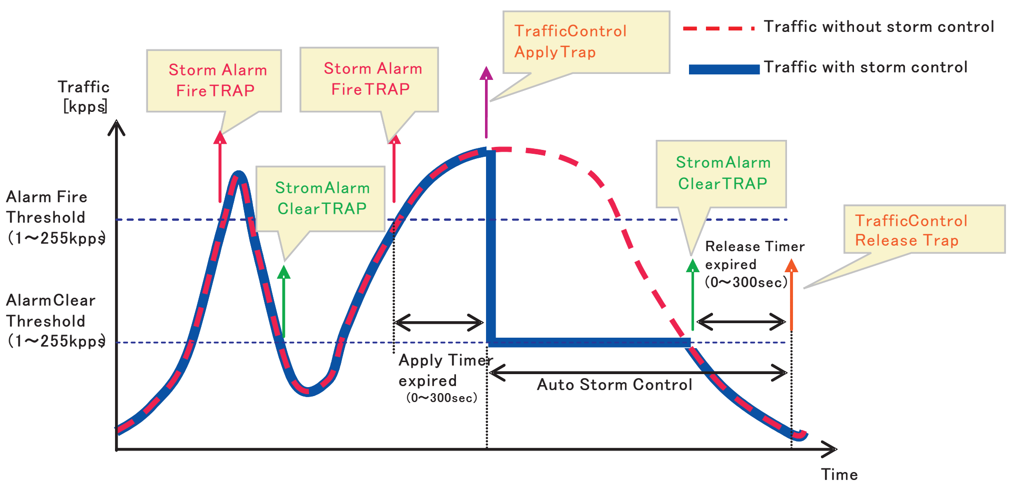
| Command | Function | Mode |
|---|---|---|
| snmp-server enable port-traps atc multicast-control-apply | Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control and the apply timer expires | IC (Port) |
| snmp-server enable port-traps atc multicast-control-release | Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires | IC (Port) |
| *ATC Display Commands* | | |
| show auto-traffic-control | Shows global configuration settings for automatic storm control | PE |
| show auto-traffic-control interface | Shows interface configuration settings and storm control status for the specified port | PE |

1. Enabling automatic storm control on a port will disable hardware-level storm control on the same port if configured by the switchport packet-rate command.

## USAGE GUIDELINES

ATC includes storm control for broadcast or multicast traffic. The control response for either of these traffic types is the same, as shown in the following diagrams.

**Figure 1: Storm Control by Limiting the Traffic Rate**

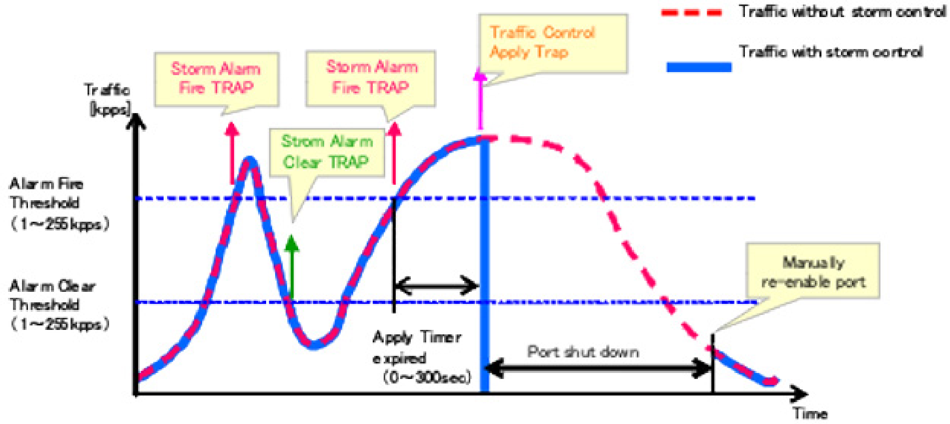



The key elements of this diagram are described below:

- Alarm Fire Threshold – The highest acceptable traffic rate. When ingress traffic exceeds the threshold, ATC sends a Storm Alarm Fire Trap and logs it.
- When traffic exceeds the alarm fire threshold and the apply timer expires, a traffic control response is applied, and a Traffic Control Apply Trap is sent and logged.
- Alarm Clear Threshold – The lower threshold beneath which an control response can be automatically terminated after the release timer expires. When ingress traffic falls below this threshold, ATC sends a Storm Alarm Clear Trap and logs it.
- When traffic falls below the alarm clear threshold after the release timer expires, traffic control will be stopped and a Traffic Control Release Trap sent and logged.

◆ The traffic control response of rate limiting can be released automatically or manually. The control response of shutting down a port can only be released manually.

**Figure 2: Storm Control by Shutting Down a Port**




The key elements of this diagram are the same as that described in the preceding diagram, except that automatic release of the control response is not provided. When traffic control is applied, you must manually re-enable the port.

#### FUNCTIONAL LIMITATIONS

Automatic storm control is a software level control function. Traffic storms can also be controlled at the hardware level using the switchport packet-rate command. However, only one of these control types can be applied to a port. Enabling automatic storm control on a port will disable hardware-level storm control on that port.

## auto-traffic-control apply-timer

This command sets the time at which to apply the control response after ingress traffic has exceeded the upper threshold. Use the **no** form to restore the default setting.

#### SYNTAX

**auto-traffic-control** {**broadcast** | **multicast**} **apply-timer** *seconds*

**no auto-traffic-control** {**broadcast** | **multicast**} **apply-timer**

**broadcast** - Specifies automatic storm control for broadcast traffic.

**multicast** - Specifies automatic storm control for multicast traffic.

*seconds* - The interval after the upper threshold has been exceeded at which to apply the control response. (Range: 1-300 seconds)

#### DEFAULT SETTING

300 seconds

#### COMMAND MODE

Global Configuration

**COMMAND USAGE**
After the apply timer expires, a control action may be triggered as specified by the auto-traffic-control action command and a trap message sent as specified by the snmp-server enable port-traps atc broadcast-control-apply command or snmp-server enable port-traps atc multicast-control-apply command.

**EXAMPLE**
This example sets the apply timer to 200 seconds for all ports.

```
Console(config)#auto-traffic-control broadcast apply-timer 200
Console(config)#
```

## auto-traffic-control release-timer

This command sets the time at which to release the control response after ingress traffic has fallen beneath the lower threshold. Use the **no** form to restore the default setting.

**SYNTAX**

**auto-traffic-control** {**broadcast** | **multicast**}
**release-timer** *seconds*

**no auto-traffic-control** {**broadcast** | **multicast**} **release-timer**

**broadcast** - Specifies automatic storm control for broadcast traffic.

**multicast** - Specifies automatic storm control for multicast traffic.

*seconds* - The time at which to release the control response after ingress traffic has fallen beneath the lower threshold. (Range: 1-900 seconds)

**DEFAULT SETTING**
900 seconds

**COMMAND MODE**
Global Configuration

**COMMAND USAGE**
This command sets the delay after which the control response can be terminated. The auto-traffic-control auto-control-release command must be used to enable or disable the automatic release.

**EXAMPLE**
This example sets the release timer to 800 seconds for all ports.

```
Console(config)#auto-traffic-control broadcast release-timer 800
Console(config)#
```

## auto-traffic-control

This command enables automatic traffic control for broadcast or multicast storms. Use the **no** form to disable this feature.

#### SYNTAX

[**no**] **auto-traffic-control** {**broadcast** | **multicast**}

**broadcast** - Specifies automatic storm control for broadcast traffic.

**multicast** - Specifies automatic storm control for multicast traffic.

#### DEFAULT SETTING

Disabled

#### COMMAND MODE

Interface Configuration (Ethernet)

#### COMMAND USAGE

- Automatic storm control can be enabled for either broadcast or multicast traffic. It cannot be enabled for both of these traffic types at the same time.
- Automatic storm control is a software level control function. Traffic storms can also be controlled at the hardware level using the switchport packet-rate command. However, only one of these control types can be applied to a port. Enabling automatic storm control on a port will disable hardware-level storm control on that port.

#### EXAMPLE

This example enables automatic storm control for broadcast traffic on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast
Console(config-if)#
```

### auto-traffic-control action

This command sets the control action to limit ingress traffic or shut down the offending port. Use the **no** form to restore the default setting.

#### SYNTAX

**auto-traffic-control** {**broadcast** | **multicast**}
**action** {**rate-control** | **shutdown**}

**no auto-traffic-control** {**broadcast** | **multicast**} **action**

**broadcast** - Specifies automatic storm control for broadcast traffic.

**multicast** - Specifies automatic storm control for multicast traffic.

**rate-control** - If a control response is triggered, the rate of ingress traffic is limited based on the threshold configured by the auto-traffic-control alarm-clear-threshold command.

**shutdown** - If a control response is triggered, the port is administratively disabled. A port disabled by automatic traffic control can only be manually re-enabled.

#### DEFAULT SETTING

rate-control

#### COMMAND MODE
Interface Configuration (Ethernet)

#### COMMAND USAGE
- When the upper threshold is exceeded and the apply timer expires, a control response will be triggered based on this command.
- When the control response is set to rate limiting by this command, the rate limits are determined by the auto-traffic-control alarm-clear-threshold command.
- If the control response is to limit the rate of ingress traffic, it can be automatically terminated once the traffic rate has fallen beneath the lower threshold and the release timer has expired.
- If a port has been shut down by a control response, it will not be re-enabled by automatic traffic control. It can only be manually re-enabled using the auto-traffic-control control-release command.

#### EXAMPLE
This example sets the control response for broadcast traffic on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast action shutdown
Console(config-if)#
```

### auto-traffic-control alarm-clear-threshold

This command sets the lower threshold for ingress traffic beneath which a cleared storm control trap is sent. Use the **no** form to restore the default setting.

#### SYNTAX

**auto-traffic-control** {**broadcast** | **multicast**}
**alarm-clear-threshold** *threshold*

**no auto-traffic-control** {**broadcast** | **multicast**}
**alarm-clear-threshold**

**broadcast** - Specifies automatic storm control for broadcast traffic.

**multicast** - Specifies automatic storm control for multicast traffic.

*threshold* - The lower threshold for ingress traffic beneath which a cleared storm control trap is sent. (Range: 1-255 kilo-packets per second seconds)

#### DEFAULT SETTING
128 kilo-packets per seconds

#### COMMAND MODE
Interface Configuration (Ethernet)

#### COMMAND USAGE
- Once the traffic rate falls beneath the lower threshold, a trap message may be sent if configured by the snmp-server enable port-traps atc broadcast-alarm-clear command or snmp-server enable port-traps atc multicast-alarm-clear command.

◆ If rate limiting has been configured as a control response, it will discontinued after the traffic rate has fallen beneath the lower threshold, and the release timer has expired. Note that if a port has been shut down by a control response, it will not be re-enabled by automatic traffic control. It can only be manually re-enabled using the auto-traffic-control control-release command.

#### EXAMPLE

This example sets the clear threshold for automatic storm control for broadcast traffic on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast alarm-clear-threshold 155
Console(config-if)#
```

## auto-traffic-control alarm-fire-threshold

This command sets the upper threshold for ingress traffic beyond which a storm control response is triggered after the apply timer expires. Use the **no** form to restore the default setting.

#### SYNTAX

**auto-traffic-control** {**broadcast** | **multicast**} **alarm-fire-threshold** *threshold*

**no auto-traffic-control** {**broadcast** | **multicast**} **alarm-fire-threshold**

**broadcast** - Specifies automatic storm control for broadcast traffic.

**multicast** - Specifies automatic storm control for multicast traffic.

*threshold* - The upper threshold for ingress traffic beyond which a storm control response is triggered after the apply timer expires. (Range: 1-255 kilo-packets per second seconds)

#### DEFAULT SETTING

128 kilo-packets per seconds

#### COMMAND MODE

Interface Configuration (Ethernet)

#### COMMAND USAGE

◆ Once the upper threshold is exceeded, a trap message may be sent if configured by the snmp-server enable port-traps atc broadcast-alarm-fire command or snmp-server enable port-traps atc multicast-alarm-fire command.

◆ After the upper threshold is exceeded, the control timer must first expire as configured by the auto-traffic-control apply-timer command before a control response is triggered if configured by the auto-traffic-control action command.

#### EXAMPLE

This example sets the trigger threshold for automatic storm control for broadcast traffic on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast alarm-fire-threshold 255
Console(config-if)#
```

## auto-traffic-control auto-control-release

This command automatically releases a control response after the time specified in the auto-traffic-control release-timer command has expired.

#### SYNTAX

**auto-traffic-control** {**broadcast** | **multicast**} **auto-control-release**

**broadcast** - Specifies automatic storm control for broadcast traffic.

**multicast** - Specifies automatic storm control for multicast traffic.

#### COMMAND MODE

Interface Configuration (Ethernet)

#### COMMAND USAGE

This command can be used to automatically stop a control response after the specified action has been triggered and the release timer has expired.

#### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast auto-control-release
Console(config-if)#
```

## auto-traffic-control control-release

This command manually releases a control response.

#### SYNTAX

**auto-traffic-control** {**broadcast** | **multicast**} **control-release**

**broadcast** - Specifies automatic storm control for broadcast traffic.

**multicast** - Specifies automatic storm control for multicast traffic.

#### COMMAND MODE

Privileged Exec

#### COMMAND USAGE

This command can be used to manually stop a control response any time after the specified action has been triggered.

### EXAMPLE

```
Console#auto-traffic-control broadcast control-release interface ethernet 1/1
Console#
```

## snmp-server enable port-traps atc broadcast-alarm-clear

This command sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered. Use the **no** form to disable this trap.

### SYNTAX

[**no**] **snmp-server enable port-traps atc broadcast-alarm-clear**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Interface Configuration (Ethernet)

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-alarm-clear
Console(config-if)#
```

### RELATED COMMANDS

auto-traffic-control action (843)
auto-traffic-control alarm-clear-threshold (844)

## snmp-server enable port-traps atc broadcast-alarm-fire

This command sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control. Use the **no** form to disable this trap.

### SYNTAX

[**no**] **snmp-server enable port-traps atc broadcast-alarm-fire**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Interface Configuration (Ethernet)

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-alarm-fire
Console(config-if)#
```

### RELATED COMMANDS

auto-traffic-control alarm-fire-threshold (845)

## snmp-server enable port-traps atc broadcast-control-apply

This command sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control and the apply timer expires. Use the **no** form to disable this trap.

### SYNTAX

[**no**] **snmp-server enable port-traps atc broadcast-control-apply**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Interface Configuration (Ethernet)

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-control-apply
Console(config-if)#
```

### RELATED COMMANDS

auto-traffic-control alarm-fire-threshold (845)
auto-traffic-control apply-timer (841)

## snmp-server enable port-traps atc broadcast-control-release

This command sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires. Use the **no** form to disable this trap.

### SYNTAX

[**no**] **snmp-server enable port-traps atc broadcast-control-release**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Interface Configuration (Ethernet)

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-control-release
Console(config-if)#
```

### RELATED COMMANDS

auto-traffic-control alarm-clear-threshold (844)

auto-traffic-control action (843)
auto-traffic-control release-timer (842)

## snmp-server enable port-traps atc multicast-alarm-clear

This command sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered. Use the **no** form to disable this trap.

### SYNTAX

[**no**] **snmp-server enable port-traps atc multicast-alarm-clear**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Interface Configuration (Ethernet)

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-alarm-clear
Console(config-if)#
```

### RELATED COMMANDS

auto-traffic-control action (843)
auto-traffic-control alarm-clear-threshold (844)

## snmp-server enable port-traps atc multicast-alarm-fire

This command sends a trap when multicast traffic exceeds the upper threshold for automatic storm control. Use the **no** form to disable this trap.

### SYNTAX

[**no**] **snmp-server enable port-traps atc multicast-alarm-fire**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Interface Configuration (Ethernet)

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-alarm-fire
Console(config-if)#
```

### RELATED COMMANDS

auto-traffic-control alarm-fire-threshold (845)

## snmp-server enable port-traps atc multicast-control-apply

This command sends a trap when multicast traffic exceeds the upper threshold for automatic storm control and the apply timer expires. Use the **no** form to disable this trap.

### SYNTAX

[**no**] **snmp-server enable port-traps atc multicast-control-apply**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Interface Configuration (Ethernet)

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-control-apply
Console(config-if)#
```

### RELATED COMMANDS

auto-traffic-control alarm-fire-threshold (845)
auto-traffic-control apply-timer (841)

## snmp-server enable port-traps atc multicast-control-release

This command sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires. Use the **no** form to disable this trap.

### SYNTAX

[**no**] **snmp-server enable port-traps atc multicast-control-release**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Interface Configuration (Ethernet)

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-control-release
Console(config-if)#
```

### RELATED COMMANDS

auto-traffic-control alarm-clear-threshold (844)
auto-traffic-control action (843)
auto-traffic-control release-timer (842)

## show auto-traffic-control

This command shows global configuration settings for automatic storm control.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show auto-traffic-control

Storm-control: Broadcast
 Apply-timer (sec)   : 300
 release-timer (sec) : 900

Storm-control: Multicast
 Apply-timer(sec)    : 300
 release-timer(sec)  : 900
Console#
```

## show auto-traffic-control interface

This command shows interface configuration settings and storm control status for the specified port.

### SYNTAX

**show auto-traffic-control interface** [*interface*]

*interface*

**ethernet** *unit*/*port*

*unit* - Unit identifier. (Range: 1-8)

*port* - Port number. (Range: 1-28)

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show auto-traffic-control interface ethernet 1/1
Eth 1/1 Information
-----------------------------------------------------------------------
Storm Control:             Broadcast                  Multicast
State:                     Disabled                   Disabled
Action:                    rate-control               rate-control
Auto Release Control:      Disabled                   Disabled
Alarm Fire Threshold(Kpps): 128                       128
Alarm Clear Threshold(Kpps):128                       128
Trap Storm Fire:           Disabled                   Disabled
Trap Storm Clear:          Disabled                   Disabled
Trap Traffic Apply:        Disabled                   Disabled
Trap Traffic Release:      Disabled                   Disabled
-----------------------------------------------------------------------

Console#
```

# 37 ADDRESS TABLE COMMANDS

These commands are used to configure the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time.

**Table 1: Address Table Commands**

| Command | Function | Mode |
|---|---|---|
| mac-address-table aging-time | Sets the aging time of the address table | GC |
| mac-address-table static | Maps a static address to a port in a VLAN | GC |
| clear mac-address-table dynamic | Removes any learned entries from the forwarding database | PE |
| show mac-address-table | Displays entries in the bridge-forwarding database | PE |
| show mac-address-table aging-time | Shows the aging time for the address table | PE |
| show mac-address-table count | Shows the number of MAC addresses used and the number of available MAC addresses | PE |

## mac-address-table aging-time

This command sets the aging time for entries in the address table. Use the **no** form to restore the default aging time.

### SYNTAX

**mac-address-table aging-time** *seconds*

**no mac-address-table aging-time**

*seconds* - Aging time. (Range: 10-1000000 seconds; 0 to disable aging)

### DEFAULT SETTING

300 seconds

### COMMAND MODE

Global Configuration

### COMMAND USAGE

The aging time is used to age out dynamically learned forwarding information.

### EXAMPLE

```
Console(config)#mac-address-table aging-time 100
Console(config)#
```

## mac-address-table static

This command maps a static address to a destination port in a VLAN. Use the **no** form to remove an address.

### SYNTAX

**mac-address-table static** *mac-address* **interface** *interface* **vlan** *vlan-id* [*action*]

**no mac-address-table static** *mac-address* **vlan** *vlan-id*

*mac-address* - MAC address.

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/181-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

*vlan-id* - VLAN ID (Range: 1-4093)

*action* -

**delete-on-reset** - Assignment lasts until the switch is reset.

**permanent** - Assignment is permanent.

### DEFAULT SETTING

No static addresses are defined. The default mode is **permanent**.

### COMMAND MODE

Global Configuration

### COMMAND USAGE

The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

- Static addresses will not be removed from the address table when a given interface link is down.
- Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.
- A static address cannot be learned on another port until the address is removed with the **no** form of this command.

### EXAMPLE

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

## clear mac-address-table dynamic

This command removes any learned entries from the forwarding database.

### DEFAULT SETTING
None

### COMMAND MODE
Privileged Exec

### EXAMPLE

```
Console#clear mac-address-table dynamic
Console#
```

## show mac-address-table

This command shows classes of entries in the bridge-forwarding database.

### SYNTAX

**show mac-address-table** [**address** *mac-address* [*mask*]] [**interface** *interface*]
[**vlan** *vlan-id*]
[**sort** {**address** | **vlan** | **interface**}]

*mac-address* - MAC address.

*mask* - Bits to match in the address.

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

*vlan-id* - VLAN ID (Range: 1-4093)

**sort** - Sort by address, vlan or interface.

### DEFAULT SETTING
None

### COMMAND MODE
Privileged Exec

### COMMAND USAGE

- The MAC Address Table contains the MAC addresses associated with each interface. Note that the Type field may include the following types:
  - Learn - Dynamic address entries
  - Config - Static entry
- 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 16K.

#### EXAMPLE

```
Console#show mac-address-table
 Interface MAC Address       VLAN Type     Life Time
 --------- ----------------- ---- -------- -----------------
  Eth 1/ 1 00-E0-29-94-34-DE    1 Config   Delete on Reset
  Eth 1/21 00-01-EC-F8-D8-D9    1 Learn    Delete on Timeout
Console#
```

### show mac-address-table aging-time

This command shows the aging time for entries in the address table.

#### DEFAULT SETTING

None

#### COMMAND MODE

Privileged Exec

#### EXAMPLE

```
Console#show mac-address-table aging-time
 Aging Status : Enabled
 Aging Time: 300 sec.
Console#
```

### show mac-address-table count

This command shows the number of MAC addresses used and the number of available MAC addresses for the overall system or for an interface.

#### SYNTAX

**show mac-address-table count** [**interface** *interface*]

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

#### DEFAULT SETTING

None

#### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show mac-address-table count

Compute the number of MAC Address...

Maximum number of MAC Address which can be created in the system:
Total Number of MAC Address      : 16384
Number of Static MAC Address     : 1024

Current number of entries which have been created in the system:
Total Number of MAC Address      : 2
Number of Static MAC Address     : 1
Number of Dynamic MAC Address    : 1

Console#show mac-address-table count interface ethernet 1/1

MAC Entries for port ID :1
 --------- ----------------- ---- --------
Dynamic Address Count  :1
Total MAC Address     :1
Total MAC Address Space Avaiable: 16384
Console#
```

# 38 SPANNING TREE COMMANDS

This section includes commands that configure the Spanning Tree Algorithm (STA) globally for the switch, and commands that configure STA for the selected interface.

**Table 1: Spanning Tree Commands**

| Command | Function | Mode |
|---|---|---|
| spanning-tree | Enables the spanning tree protocol | GC |
| spanning-tree forward-time | Configures the spanning tree bridge forward time | GC |
| spanning-tree hello-time | Configures the spanning tree bridge hello time | GC |
| spanning-tree max-age | Configures the spanning tree bridge maximum age | GC |
| spanning-tree mode | Configures STP, RSTP or MSTP mode | GC |
| spanning-tree pathcost method | Configures the path cost method for RSTP/MSTP | GC |
| spanning-tree priority | Configures the spanning tree bridge priority | GC |
| spanning-tree mst configuration | Changes to MSTP configuration mode | GC |
| spanning-tree system-bpdu-flooding | Floods BPDUs to all other ports or just to all other ports in the same VLAN when global spanning tree is disabled | GC |
| spanning-tree transmission-limit | Configures the transmission limit for RSTP/MSTP | GC |
| max-hops | Configures the maximum number of hops allowed in the region before a BPDU is discarded | MST |
| mst priority | Configures the priority of a spanning tree instance | MST |
| mst vlan | Adds VLANs to a spanning tree instance | MST |
| name | Configures the name for the multiple spanning tree | MST |
| revision | Configures the revision number for the multiple spanning tree | MST |
| spanning-tree bpdu-filter | Filters BPDUs for edge ports | IC |
| spanning-tree bpdu-guard | Shuts down an edge port if it receives a BPDU | IC |
| spanning-tree cost | Configures the spanning tree path cost of an interface | IC |
| spanning-tree edge-port | Enables fast forwarding for edge ports | IC |
| spanning-tree link-type | Configures the link type for RSTP/MSTP | IC |
| spanning-tree loopback-detection | Enables BPDU loopback detection for a port | IC |
| spanning-tree loopback-detection release-mode | Configures loopback release mode for a port | IC |
| spanning-tree loopback-detection trap | Enables BPDU loopback SNMP trap notification for a port | IC |
| spanning-tree mst cost | Configures the path cost of an instance in the MST | IC |
| spanning-tree mst port-priority | Configures the priority of an instance in the MST | IC |

**Table 1: Spanning Tree Commands (Continued)**

| Command | Function | Mode |
|---|---|---|
| spanning-tree port-bpdu-flooding | Floods BPDUs to other ports when global spanning tree is disabled | IC |
| spanning-tree port-priority | Configures the spanning tree priority of an interface | IC |
| spanning-tree root-guard | Prevents a designated port from passing superior BPDUs | IC |
| spanning-tree spanning-disabled | Disables spanning tree for an interface | IC |
| spanning-tree loopback-detection release | Manually releases a port placed in discarding state by loopback-detection | PE |
| spanning-tree protocol-migration | Re-checks the appropriate BPDU format | PE |
| show spanning-tree | Shows spanning tree configuration for the common spanning tree (i.e., overall bridge), a selected interface, or an instance within the multiple spanning tree | PE |
| show spanning-tree mst configuration | Shows the multiple spanning tree configuration | PE |

## spanning-tree

This command enables the Spanning Tree Algorithm globally for the switch. Use the **no** form to disable it.

### SYNTAX

[**no**] **spanning-tree**

### DEFAULT SETTING

Spanning tree is enabled.

### COMMAND MODE

Global Configuration

### COMMAND USAGE

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

### EXAMPLE

This example shows how to enable the Spanning Tree Algorithm for the switch:

```
Console(config)#spanning-tree
Console(config)#
```

## spanning-tree 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)#
```

### RELATED COMMANDS

spanning-tree forward-time (861)
spanning-tree max-age (862)

## spanning-tree max-age

This command configures the spanning tree bridge maximum age globally for this switch. Use the **no** form to restore the default.

### SYNTAX

**spanning-tree max-age** *seconds*

**no spanning-tree max-age**

*seconds* - Time in seconds. (Range: 6-40 seconds)
The minimum value is the higher of 6 or [2 x (hello-time + 1)].
The maximum value is the lower of 40 or [2 x (forward-time - 1)].

### DEFAULT SETTING

20 seconds

### COMMAND MODE

Global Configuration

### COMMAND USAGE

This command sets the maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

### EXAMPLE

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

### RELATED COMMANDS

spanning-tree forward-time (861)
spanning-tree hello-time (861)

## spanning-tree mode

This command selects the spanning tree mode for this switch. Use the **no** form to restore the default.

### SYNTAX

**spanning-tree mode** {**stp** | **rstp** | **mstp**}

**no spanning-tree mode**

**stp** - Spanning Tree Protocol (IEEE 802.1D)

**rstp** - Rapid Spanning Tree Protocol (IEEE 802.1w)

**mstp** - Multiple Spanning Tree (IEEE 802.1s)

### DEFAULT SETTING

rstp

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- Spanning Tree Protocol
  Uses RSTP for the internal state machine, but sends only 802.1D BPDUs. This creates one spanning tree instance for the entire network. If multiple VLANs are implemented on a network, the path between specific VLAN members may be inadvertently disabled to prevent network loops, thus isolating group members. When operating multiple VLANs, we recommend selecting the MSTP option.

- Rapid Spanning Tree Protocol
  RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:

  - STP Mode – If the switch receives an 802.1D BPDU after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.

  - RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

- Multiple Spanning Tree Protocol

  - To allow multiple spanning trees to operate over the network, you must configure a related set of bridges with the same MSTP configuration, allowing them to participate in a specific set of spanning tree instances.

  - A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments.

  - Be careful when switching between spanning tree modes. Changing modes stops all spanning-tree instances for the previous mode and restarts the system in the new mode, temporarily disrupting user traffic.

### EXAMPLE

The following example configures the switch to use Rapid Spanning Tree:

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

## spanning-tree pathcost method

This command configures the path cost method used for Rapid Spanning Tree and Multiple Spanning Tree. Use the **no** form to restore the default.

### SYNTAX

**spanning-tree pathcost method** {**long** | **short**}

**no spanning-tree pathcost method**

**long** - Specifies 32-bit based values that range from 1-200,000,000. This method is based on the IEEE 802.1w Rapid Spanning Tree Protocol.

**short** - Specifies 16-bit based values that range from 1-65535. This method is based on the IEEE 802.1 Spanning Tree Protocol.

### DEFAULT SETTING

Long method

### COMMAND MODE

Global Configuration

### COMMAND USAGE

The path cost method is used to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Note that path cost (page 871) takes precedence over port priority (page 878).

### EXAMPLE

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

## spanning-tree priority

This command configures the spanning tree priority globally for this switch. Use the **no** form to restore the default.

### SYNTAX

**spanning-tree priority** *priority*

**no spanning-tree priority**

*priority* - Priority of the bridge. (Range – 0-61440, in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

#### DEFAULT SETTING

32768

#### COMMAND MODE

Global Configuration

#### COMMAND USAGE

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority (i.e., lower numeric value) becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

#### EXAMPLE

```
Console(config)#spanning-tree priority 40000
Console(config)#
```

### spanning-tree mst configuration

This command changes to Multiple Spanning Tree (MST) configuration mode.

#### DEFAULT SETTING

No VLANs are mapped to any MST instance.
The region name is set the switch's MAC address.

#### COMMAND MODE

Global Configuration

#### EXAMPLE

```
Console(config)#spanning-tree mst configuration
Console(config-mstp)#
```

#### RELATED COMMANDS

mst vlan (868)
mst priority (867)
name (869)
revision (869)
max-hops (867)

## spanning-tree system-bpdu-flooding

This command configures the system to flood BPDUs to all other ports on the switch or just to all other ports in the same VLAN when spanning tree is disabled globally on the switch or disabled on a specific port. Use the **no** form to restore the default.

### SYNTAX

**spanning-tree system-bpdu-flooding** {**to-all** | **to-vlan**}

**no spanning-tree system-bpdu-flooding**

**to-all** - Floods BPDUs to all other ports on the switch.

**to-vlan** - Floods BPDUs to all other ports within the receiving port's native VLAN (i.e., as determined by port's PVID).

### DEFAULT SETTING

Floods to all other ports in the same VLAN.

### COMMAND MODE

Global Configuration

### COMMAND USAGE

The **spanning-tree system-bpdu-flooding** command has no effect if BPDU flooding is disabled on a port (see the spanning-tree port-bpdu-flooding command).

### EXAMPLE

```
Console(config)#spanning-tree system-bpdu-flooding
Console(config)#
```

## spanning-tree transmission-limit

This command configures the minimum interval between the transmission of consecutive RSTP/MSTP BPDUs. Use the **no** form to restore the default.

### SYNTAX

**spanning-tree transmission-limit** *count*

**no spanning-tree transmission-limit**

*count* - The transmission limit in seconds. (Range: 1-10)

### DEFAULT SETTING

3

### COMMAND MODE

Global Configuration

### COMMAND USAGE

This command limits the maximum transmission rate for BPDUs.

#### EXAMPLE

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

### max-hops

This command configures the maximum number of hops in the region before a BPDU is discarded. Use the **no** form to restore the default.

#### SYNTAX

**max-hops** *hop-number*

*hop-number* - Maximum hop number for multiple spanning tree. (Range: 1-40)

#### DEFAULT SETTING

20

#### COMMAND MODE

MST Configuration

#### COMMAND USAGE

An MSTI region is treated as a single node by the STP and RSTP protocols. Therefore, the message age for BPDUs inside an MSTI region is never changed. However, each spanning tree instance within a region, and the internal spanning tree (IST) that connects these instances use a hop count to specify the maximum number of bridges that will propagate a BPDU. Each bridge decrements the hop count by one before passing on the BPDU. When the hop count reaches zero, the message is dropped.

#### EXAMPLE

```
Console(config-mstp)#max-hops 30
Console(config-mstp)#
```

### mst priority

This command configures the priority of a spanning tree instance. Use the **no** form to restore the default.

#### SYNTAX

**mst** *instance-id* **priority** *priority*

**no mst** *instance-id* **priority**

*instance-id* - Instance identifier of the spanning tree. (Range: 0-4094)

*priority* - Priority of the a spanning tree instance. (Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

#### DEFAULT SETTING
32768

#### COMMAND MODE
MST Configuration

#### COMMAND USAGE
- MST priority is used in selecting the root bridge and alternate bridge of the specified instance. The device with the highest priority (i.e., lowest numerical value) becomes the MSTI root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

- You can set this switch to act as the MSTI root device by specifying a priority of 0, or as the MSTI alternate device by specifying a priority of 16384.

#### EXAMPLE

```
Console(config-mstp)#mst 1 priority 4096
Console(config-mstp)#
```

### mst vlan

This command adds VLANs to a spanning tree instance. Use the **no** form to remove the specified VLANs. Using the **no** form without any VLAN parameters to remove all VLANs.

#### SYNTAX

[**no**] **mst** *instance-id* **vlan** *vlan-range*

*instance-id* - Instance identifier of the spanning tree. (Range: 0-4094)

*vlan-range* - Range of VLANs. (Range: 1-4093)

#### DEFAULT SETTING
none

#### COMMAND MODE
MST Configuration

#### COMMAND USAGE
- Use this command to group VLANs into spanning tree instances. MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.

- By default all VLANs are assigned to the Internal Spanning Tree (MSTI 0) that connects all bridges and LANs within the MST region. This switch supports up to 33 instances. You should try to group VLANs which cover the same general area of your network. However, remember that you must configure all bridges within the same MSTI Region (page 869) with the same set of instances, and the same instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each MSTI region as a single node, connecting all regions to the Common Spanning Tree.

#### EXAMPLE

```
Console(config-mstp)#mst 1 vlan 2-5
Console(config-mstp)#
```

### name

This command configures the name for the multiple spanning tree region in which this switch is located. Use the **no** form to clear the name.

#### SYNTAX

**name** *name*

*name* - Name of the spanning tree.

#### DEFAULT SETTING

Switch's MAC address

#### COMMAND MODE

MST Configuration

#### COMMAND USAGE

The MST region name and revision number (page 869) are used to designate a unique MST region. A bridge (i.e., spanning-tree compliant device such as this switch) can only belong to one MST region. And all bridges in the same region must be configured with the same MST instances.

#### EXAMPLE

```
Console(config-mstp)#name R&D
Console(config-mstp)#
```

#### RELATED COMMANDS

revision (869)

### revision

This command configures the revision number for this multiple spanning tree configuration of this switch. Use the **no** form to restore the default.

#### SYNTAX

**revision** *number*

*number* - Revision number of the spanning tree. (Range: 0-65535)

#### DEFAULT SETTING

0

#### COMMAND MODE
MST Configuration

#### COMMAND USAGE
The MST region name (page 869) and revision number are used to designate a unique MST region. A bridge (i.e., spanning-tree compliant device such as this switch) can only belong to one MST region. And all bridges in the same region must be configured with the same MST instances.

#### EXAMPLE

```
Console(config-mstp)#revision 1
Console(config-mstp)#
```

#### RELATED COMMANDS
name (869)

## spanning-tree bpdu-filter

This command filters all BPDUs received on an edge port. Use the **no** form to disable this feature.

#### SYNTAX

[**no**] **spanning-tree bpdu-filter**

#### DEFAULT SETTING
Disabled

#### COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

#### COMMAND USAGE
- This command filters all Bridge Protocol Data Units (BPDUs) received on an interface to save CPU processing time. This function is designed to work in conjunction with edge ports which should only connect end stations to the switch, and therefore do not need to process BPDUs. However, note that if a trunking port connected to another switch or bridging device is mistakenly configured as an edge port, and BPDU filtering is enabled on this port, this might cause a loop in the spanning tree.
- Before enabling BPDU Filter, the interface must first be configured as an edge port with the spanning-tree edge-port command.

#### EXAMPLE

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree bpdu-filter
Console(config-if)#
```

#### RELATED COMMANDS
spanning-tree edge-port (873)

## spanning-tree bpdu-guard

This command shuts down an edge port (i.e., an interface set for fast forwarding) if it receives a BPDU. Use the **no** form to disable this feature.

### SYNTAX

[**no**] **spanning-tree bpdu-guard**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE

- An edge port should only be connected to end nodes which do not generate BPDUs. If a BPDU is received on an edge port, this indicates an invalid network configuration, or that the switch may be under attack by a hacker. If an interface is shut down by BPDU Guard, it must be manually re-enabled using the no spanning-tree spanning-disabled command.

- Before enabling BPDU Guard, the interface must be configured as an edge port with the spanning-tree edge-port command. Also note that if the edge port attribute is disabled on an interface, BPDU Guard will also be disabled on that interface.

### EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree bpdu-guard
Console(config-if)#
```

### RELATED COMMANDS

spanning-tree edge-port (873)
spanning-tree spanning-disabled (880)

## spanning-tree cost

This command configures the spanning tree path cost for the specified interface. Use the **no** form to restore the default auto-configuration mode.

### SYNTAX

**spanning-tree cost** *cost*

**no spanning-tree cost**

*cost* - The path cost for the port. (Range: 0 for auto-configuration, 1-65535 for short path cost method[1], 1-200,000,000 for long path cost method)

**Table 2: Recommended STA Path Cost Range**

| Port Type | Short Path Cost (IEEE 802.1D-1998) | Long Path Cost (802.1D-2004) |
|---|---|---|
| Fast Ethernet | 10-60 | 20,000-2,000,000 |
| Gigabit Ethernet | 3-10 | 2,000-200,000 |
| 10G Ethernet | 200-20,000 | 200-20,000 |

### DEFAULT SETTING

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost “0” is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

**Table 3: Default STA Path Costs**

| Port Type | Short Path Cost (IEEE 802.1D-1998) | Long Path Cost (802.1D-2004) |
|---|---|---|
| Fast Ethernet | 100,000 | 100,000 |
| Gigabit Ethernet | 10,000 | 10,000 |
| 10G Ethernet | 1,000 | 1,000 |

### 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.
- Path cost takes precedence over port priority.
- When the path cost method (page 864) is set to short, the maximum value for path cost is 65,535.

### EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

1. Use the spanning-tree pathcost method command on page 864 to set the path cost method.

## 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 time out problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.

### EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

## spanning-tree link-type

This command configures the link type for Rapid Spanning Tree and Multiple Spanning Tree. Use the **no** form to restore the default.

### SYNTAX

**spanning-tree link-type** {**auto** | **point-to-point** | **shared**}

**no spanning-tree link-type**

- **auto** - Automatically derived from the duplex mode setting.
- **point-to-point** - Point-to-point link.
- **shared** - Shared medium.

### DEFAULT SETTING

auto

### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE

- Specify a point-to-point link if the interface can only be connected to exactly one other bridge, or a shared link if it can be connected to two or more bridges.
- When automatic detection is selected, the switch derives the link type from the duplex mode. A full-duplex interface is considered a point-to-point link, while a half-duplex interface is assumed to be on a shared link.
- RSTP only works on point-to-point links between two bridges. If you designate a port as a shared link, RSTP is forbidden. Since MSTP is an extension of RSTP, this same restriction applies.

### EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree link-type point-to-point
```

## spanning-tree loopback-detection

This command enables the detection and response to Spanning Tree loopback BPDU packets on the port. Use the **no** form to disable this feature.

### SYNTAX

[**no**] **spanning-tree loopback-detection**

### DEFAULT SETTING

Enabled

### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE

- If Port Loopback Detection is not enabled and a port receives it's own BPDU, then the port will drop the loopback BPDU according to IEEE Standard 802.1W-2001 9.3.4 (Note 1).
- Port Loopback Detection will not be active if Spanning Tree is disabled on the switch.

### EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection
```

## spanning-tree loopback-detection release-mode

This command configures the release mode for a port that was placed in the discarding state because a loopback BPDU was received. Use the **no** form to restore the default.

### SYNTAX

**spanning-tree loopback-detection release-mode**
{**auto** | **manual**}

**no spanning-tree loopback-detection release-mode**

**auto** - Allows a port to automatically be released from the discarding state when the loopback state ends.

**manual** - The port can only be released from the discarding state manually.

### DEFAULT SETTING

auto

### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE

- If the port is configured for automatic loopback release, then the port will only be returned to the forwarding state if one of the following conditions is satisfied:
  - The port receives any other BPDU except for it's own, or;
  - The port's link status changes to link down and then link up again, or;
  - The port ceases to receive it's own BPDUs in a forward delay interval.
- If Port Loopback Detection is not enabled and a port receives it's own BPDU, then the port will drop the loopback BPDU according to IEEE Standard 802.1W-2001 9.3.4 (Note 1).
- Port Loopback Detection will not be active if Spanning Tree is disabled on the switch.
- When configured for manual release mode, then a link down / up event will not release the port from the discarding state. It can only be released using the spanning-tree loopback-detection release command.

### EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection release-mode manual
Console(config-if)#
```

## spanning-tree loopback-detection trap

This command enables SNMP trap notification for Spanning Tree loopback BPDU detections. Use the **no** form to restore the default.

### SYNTAX

[**no**] **spanning-tree loopback-detection trap**

### DEFAULT SETTING

Disabled

### COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

### EXAMPLE

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree loopback-detection trap
```

## spanning-tree mst cost

This command configures the path cost on a spanning instance in the Multiple Spanning Tree. Use the **no** form to restore the default auto-configuration mode.

### SYNTAX

**spanning-tree mst** *instance-id* **cost** *cost*

**no spanning-tree mst** *instance-id* **cost**

*instance-id* - Instance identifier of the spanning tree. (Range: 0-4094, no leading zeroes)

*cost* - Path cost for an interface. (Range: 0 for auto-configuration, 1-65535 for short path cost method[2], 1-200,000,000 for long path cost method)

The recommended path cost range is listed in Table 2 on page 872.

### DEFAULT SETTING
By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535. The default path costs are listed in Table 3 on page 872.

### COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE
- Each spanning-tree instance is associated with a unique set of VLAN IDs.
- This command is used by the multiple spanning-tree algorithm to determine the best path between devices. Therefore, lower values should be assigned to interfaces attached to faster media, and higher values assigned to interfaces with slower media.
- Use the **no spanning-tree mst cost** command to specify auto-configuration mode.
- Path cost takes precedence over interface priority.

2. Use the spanning-tree pathcost method command to set the path cost method.

### EXAMPLE

```
Console(config)#interface Ethernet 1/5
Console(config-if)#spanning-tree mst 1 cost 50
Console(config-if)#
```

### RELATED COMMANDS

spanning-tree mst port-priority (877)

## spanning-tree mst port-priority

This command configures the interface priority on a spanning instance in the Multiple Spanning Tree. Use the **no** form to restore the default.

### SYNTAX

**spanning-tree mst** *instance-id* **port-priority** *priority*

**no spanning-tree mst** ***instance-id*** **port-priority**

*instance-id* - Instance identifier of the spanning tree. (Range: 0-4094, no leading zeroes)

*priority* - Priority for an interface. (Range: 0-240 in steps of 16)

### DEFAULT SETTING

128

### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE

- This command defines the priority for the use of an interface in the multiple spanning-tree. If the path cost for all interfaces on a switch are the same, the interface with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- Where more than one interface is assigned the highest priority, the interface with lowest numeric identifier will be enabled.

### EXAMPLE

```
Console(config)#interface Ethernet 1/5
Console(config-if)#spanning-tree mst 1 port-priority 0
Console(config-if)#
```

### RELATED COMMANDS

spanning-tree mst cost (876)

## spanning-tree port-bpdu-flooding

This command floods BPDUs to other ports when spanning tree is disabled globally or disabled on a specific port. Use the **no** form to restore the default setting.

#### SYNTAX

[**no**] **spanning-tree port-bpdu-flooding**

#### DEFAULT SETTING

Enabled

#### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

#### COMMAND USAGE

- When enabled, BPDUs are flooded to all other ports on the switch or to all other ports within the receiving port's native VLAN as specified by the spanning-tree system-bpdu-flooding command.
- The spanning-tree system-bpdu-flooding command has no effect if BPDU flooding is disabled on a port by the **spanning-tree port-bpdu-flooding** command.

#### EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-bpdu-flooding
Console(config-if)#
```

### spanning-tree port-priority

This command configures the priority for the specified interface. Use the **no** form to restore the default.

#### SYNTAX

**spanning-tree port-priority** *priority*

**no spanning-tree port-priority**

*priority* - The priority for a port. (Range: 0-240, in steps of 16)

#### DEFAULT SETTING

128

#### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

#### COMMAND USAGE

- This command defines the priority for the use of a port in the Spanning Tree Algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

### EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 0
```

### RELATED COMMANDS

spanning-tree cost (871)

## spanning-tree root-guard

This command prevents a designated port[3] from taking superior BPDUs into account and allowing a new STP root port to be elected. Use the **no** form to disable this feature.

### SYNTAX

[**no**] **spanning-tree root-guard**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE

- A bridge with a lower bridge identifier (or same identifier and lower MAC address) can take over as the root bridge at any time.
- When Root Guard is enabled, and the switch receives a superior BPDU on this port, it is set to the Discarding state until it stops receiving superior BPDUs for a fixed recovery period. While in the discarding state, no traffic is forwarded across the port.
- Root Guard can be used to ensure that the root bridge is not formed at a suboptimal location. Root Guard should be enabled on any designated port connected to low-speed bridges which could potentially overload a slower link by taking over as the root port and forming a new spanning tree topology. It could also be used to form a border around part of the network where the root bridge is allowed.
- When spanning tree is initialized globally on the switch or on an interface, the switch will wait for 20 seconds to ensure that the spanning tree has converged before enabling Root Guard.

### EXAMPLE

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree root-guard
Console(config-if)#
```

3. See Port Role under ?$paratext>? on page 190.

## spanning-tree spanning-disabled

This command disables the spanning tree algorithm for the specified interface. Use the **no** form to re-enable the spanning tree algorithm for the specified interface.

### SYNTAX

[**no**] **spanning-tree spanning-disabled**

### DEFAULT SETTING

Enabled

### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

### EXAMPLE

This example disables the spanning tree algorithm for port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree spanning-disabled
Console(config-if)#
```

## spanning-tree loopback-detection release

This command manually releases a port placed in discarding state by loopback-detection.

### SYNTAX

**spanning-tree loopback-detection release** *interface*

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

### COMMAND MODE

Privileged Exec

### COMMAND USAGE

Use this command to release an interface from discarding state if loopback detection release mode is set to “manual” by the spanning-tree loopback-detection release-mode command and BPDU loopback occurs.

### EXAMPLE

```
Console#spanning-tree loopback-detection release ethernet 1/1
Console#
```

## spanning-tree protocol-migration

This command re-checks the appropriate BPDU format to send on the selected interface.

### SYNTAX

**spanning-tree protocol-migration** *interface*

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

### COMMAND MODE

Privileged Exec

### COMMAND USAGE

If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the **spanning-tree protocol-migration** command at any time to manually re-check the appropriate BPDU format to send on the selected interfaces (i.e., RSTP or STP-compatible).

### EXAMPLE

```
Console#spanning-tree protocol-migration eth 1/5
Console#
```

## show spanning-tree

This command shows the configuration for the common spanning tree (CST) or for an instance within the multiple spanning tree (MST).

### SYNTAX

**show spanning-tree** [*interface* | **mst** *instance-id*]

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

*instance-id* - Instance identifier of the multiple spanning tree. (Range: 0-4094, no leading zeroes)

### DEFAULT SETTING

None

### COMMAND MODE

Privileged Exec

### COMMAND USAGE

- Use the **show spanning-tree** command with no parameters to display the spanning tree configuration for the switch for the Common Spanning Tree (CST) and for every interface in the tree.
- Use the **show spanning-tree** *interface* command to display the spanning tree configuration for an interface within the Common Spanning Tree (CST).
- Use the **show spanning-tree mst** *instance-id* command to display the spanning tree configuration for an instance within the Multiple Spanning Tree (MST).
- For a description of the items displayed under "Spanning-tree information," see ?$paratext>? on page 181. For a description of the items displayed for specific interfaces, see ?$paratext>? on page 190.

### EXAMPLE

```
Console#show spanning-tree
Spanning Tree Information
---------------------------------------------------------------
 Spanning Tree Mode                 : MSTP
 Spanning Tree Enabled/Disabled  : Enabled
 Instance                          : 0
 VLANs Configuration               : 1-4093
 Priority                          : 32768
 Bridge Hello Time (sec.)          : 2
 Bridge Max. Age (sec.)            : 20
 Bridge Forward Delay (sec.)       : 15
 Root Hello Time (sec.)            : 2
 Root Max. Age (sec.)              : 20
 Root Forward Delay (sec.)         : 15
 Max. Hops                         : 20
 Remaining Hops                    : 20
 Designated Root                   : 32768.0.0001ECF8D8C6
 Current Root Port                 : 21
 Current Root Cost                 : 100000
 Number of Topology Changes        : 5
 Last Topology Change Time (sec.): 11409
 Transmission Limit                : 3
 Path Cost Method                  : Long
---------------------------------------------------------------
Eth  1/ 1 information
---------------------------------------------------------------
 Admin Status                      : Enabled
 Role                              : Disabled
 State                             : Discarding
 External Admin Path Cost          : 0
 Internal Admin Path Cost          : 0
 External Oper Path Cost           : 100000
 Internal Oper Path Cost           : 100000
 Priority                          : 128
 Designated Cost                   : 100000
 Designated Port                   : 128.1
 Designated Root                   : 32768.0.0001ECF8D8C6
 Designated Bridge                 : 32768.0.123412341234
 Fast Forwarding                   : Disabled
 Forward Transitions               : 4
 Admin Edge Port                   : Disabled
 Oper Edge Port                    : Disabled
 Admin Link Type                   : Auto
 Oper Link Type                    : Point-to-point
 Spanning-Tree Status              : Enabled
```

```
Loopback Detection Status      : Enabled
Loopback Detection Release Mode : Auto
Loopback Detection Trap        : Disabled
Root Guard Status              : Disabled
BPDU Guard Status              : Disabled
BPDU Filter Status             : Disabled
.
.
.
```

## show spanning-tree mst configuration

This command shows the configuration of the multiple spanning tree.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show spanning-tree mst configuration
Mstp Configuration Information
--------------------------------------------------------------
 Configuration Name : R&D
 Revision Level     :0

 Instance VLANs
--------------------------------------------------------------
    0    1-4093
Console#
```

# 39 VLAN COMMANDS

A VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. This section describes commands used to create VLAN groups, add port members, specify how VLAN tagging is used, and enable automatic VLAN registration for the selected interface.

**Table 1: VLAN Commands**

| Command Group | Function |
|---|---|
| GVRP and Bridge Extension Commands | Configures GVRP settings that permit automatic VLAN learning; shows the configuration for bridge extension MIB |
| Editing VLAN Groups | Sets up VLAN groups, including name, VID and state |
| Configuring VLAN Interfaces | Configures VLAN interface parameters, including ingress and egress tagging mode, ingress filtering, PVID, and GVRP |
| Displaying VLAN Information | Displays VLAN groups, status, port members, and MAC addresses |
| Configuring IEEE 802.1Q Tunneling | Configures 802.1Q Tunneling (QinQ Tunneling) |
| Configuring Port-based Traffic Segmentation | Configures traffic segmentation for different client sessions based on specified downlink and uplink ports |
| Configuring Private VLANs | Configures private VLANs, including uplink and downlink ports |
| Configuring Protocol-based VLANs | Configures protocol-based VLANs based on frame type and protocol |
| Configuring IP Subnet VLANs | Configures IP Subnet-based VLANs |
| Configuring MAC Based VLANs | Configures MAC-based VLANs |
| Configuring Voice VLANs | Configures VoIP traffic detection and enables a Voice VLAN |

## GVRP and Bridge Extension Commands

GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network. This section describes how to enable GVRP for individual interfaces and globally for the switch, as well as how to display default configuration settings for the Bridge Extension MIB.

**Table 2: GVRP and Bridge Extension Commands**

| Command | Function | Mode |
|---|---|---|
| bridge-ext gvrp | Enables GVRP globally for the switch | GC |
| garp timer | Sets the GARP timer for the selected function | IC |
| switchport forbidden vlan | Configures forbidden VLANs for an interface | IC |
| switchport gvrp | Enables GVRP for an interface | IC |
| show bridge-ext | Shows the global bridge extension configuration | PE |
| show garp timer | Shows the GARP timer for the selected function | NE, PE |
| show gvrp configuration | Displays GVRP configuration for the selected interface | NE, PE |

### bridge-ext gvrp

This command enables GVRP globally for the switch. Use the **no** form to disable it.

#### Syntax

[**no**] **bridge-ext gvrp**

#### Default Setting

Disabled

#### Command Mode

Global Configuration

#### Command Usage

GVRP defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. This function should be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

#### Example

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

## garp timer

This command sets the values for the join, leave and leaveall timers. Use the **no** form to restore the timers' default values.

### SYNTAX

**garp timer** {**join** | **leave** | **leaveall**} *timer-value*

**no garp timer** {**join** | **leave** | **leaveall**}

{**join** | **leave** | **leaveall**} - Timer to set.

*timer-value* - Value of timer.
Ranges:
join: 20-1000 centiseconds
leave: 60-3000 centiseconds
leaveall: 500-18000 centiseconds

### DEFAULT SETTING

join: 20 centiseconds
leave: 60 centiseconds
leaveall: 1000 centiseconds

### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE

- Group Address Registration Protocol is used by GVRP and GMRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GMRP or GVRP registration/deregistration.
- Timer values are applied to GVRP for all the ports on all VLANs.
- Timer values must meet the following restrictions:
  - leave >= (2 x join)
  - leaveall > leave

**NOTE:** Set GVRP timers on all Layer 2 devices connected in the same network to the same values. Otherwise, GVRP may not operate successfully.

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#garp timer join 100
Console(config-if)#
```

### RELATED COMMANDS

show garp timer (889)

## 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: 1-4093).

### Default Setting

No VLANs are included in the forbidden list.

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- This command prevents a VLAN from being automatically added to the specified interface via GVRP.
- If a VLAN has been added to the set of allowed VLANs for an interface, then you cannot add it to the set of forbidden VLANs for that same interface.

### Example

The following example shows how to prevent port 1 from being added to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```

## switchport gvrp

This command enables GVRP for a port. Use the **no** form to disable it.

### Syntax

[**no**] **switchport gvrp**

### Default Setting

Disabled

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport gvrp
Console(config-if)#
```

## show bridge-ext

This command shows the configuration for bridge extension commands.

### DEFAULT SETTING
None

### COMMAND MODE
Privileged Exec

### COMMAND USAGE
See Displaying Bridge Extension Capabilities for a description of the displayed items.

### EXAMPLE

```
Console#show bridge-ext
 Maximum Supported VLAN Numbers        : 4093
 Maximum Supported VLAN ID             : 4093
 Extended Multicast Filtering Services : No
 Static Entry Individual Port          : Yes
 VLAN Learning                         : IVL
 Configurable PVID Tagging             : Yes
 Local VLAN Capable                    : No
 Traffic Classes                       : Enabled
 Global GVRP Status                    : Disabled
 GMRP                                  : Disabled
Console#
```

## show garp timer

This command shows the GARP timers for the selected interface.

### SYNTAX

**show garp timer** [*interface*]

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

### DEFAULT SETTING
Shows all GARP timers.

### COMMAND MODE
Normal Exec, Privileged Exec

### EXAMPLE

```
Console#show garp timer ethernet 1/1
Eth 1/ 1 GARP Timer Status:
 Join Timer      : 20 centiseconds
 Leave Timer     : 60 centiseconds
 Leave All Timer : 1000 centiseconds

Console#
```

### RELATED COMMANDS

garp timer (887)

## show gvrp configuration

This command shows if GVRP is enabled.

### SYNTAX

**show gvrp configuration** [*interface*]

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

### DEFAULT SETTING

Shows both global and interface-specific configuration.

### COMMAND MODE

Normal Exec, Privileged Exec

### EXAMPLE

```
Console#show gvrp configuration ethernet 1/7
Eth 1/ 7:
 GVRP Configuration : Disabled
Console#
```

# EDITING VLAN GROUPS

**Table 3: Commands for Editing VLAN Groups**

| Command | Function | Mode |
|---|---|---|
| vlan database | Enters VLAN database mode to add, change, and delete VLANs | GC |
| vlan | Configures a VLAN, including VID, name and state | VC |

**vlan database** This command enters VLAN database mode. All commands in this mode will take effect immediately.

#### DEFAULT SETTING
None

#### COMMAND MODE
Global Configuration

#### COMMAND USAGE
- Use the VLAN database command mode to add, change, and delete VLANs. After finishing configuration changes, you can display the VLAN settings by entering the show vlan command.

- Use the interface vlan command mode to define the port membership mode and add or remove ports from a VLAN. The results of these commands are written to the running-configuration file, and you can display this file by entering the show running-config command.

#### EXAMPLE

```
Console(config)#vlan database
Console(config-vlan)#
```

#### RELATED COMMANDS
show vlan (898)

**vlan** This command configures a VLAN. Use the **no** form to restore the default settings or delete a VLAN.

#### SYNTAX

**vlan** *vlan-id* [**name** *vlan-name*] **media ethernet**
[**state** {**active** | **suspend**}]

**no vlan** *vlan-id* [**name** | **state**]

*vlan-id* - VLAN ID, specified as a single number, a range of consecutive numbers separated by a hyphen, or multiple numbers separated by commas. (Range: 1-4093, 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 4093 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)#
```

#### RELATED COMMANDS

show vlan (898)

## CONFIGURING VLAN INTERFACES

**Table 4: Commands for Configuring VLAN Interfaces**

| Command | Function | Mode |
|---|---|---|
| interface vlan | Enters interface configuration mode for a specified VLAN | GC |
| switchport acceptable-frame-types | Configures frame types to be accepted by an interface | IC |
| switchport allowed vlan | Configures the VLANs associated with an interface | IC |
| switchport forbidden vlan | Configures forbidden VLANs for an interface | IC |
| switchport gvrp | Enables GVRP for an interface | IC |
| switchport ingress-filtering | Enables ingress filtering on an interface | IC |
| switchport mode | Configures VLAN membership mode for an interface | IC |
| switchport native vlan | Configures the PVID (native VLAN) of an interface | IC |
| switchport priority default | Sets a port priority for incoming untagged frames | IC |
| vlan-trunking | Allows unknown VLANs to cross the switch | IC |

### interface vlan

This command enters interface configuration mode for VLANs, which is used to configure VLAN parameters for a physical interface. Use the **no** form to change a Layer 3 normal VLAN back to a Layer 2 interface.

#### SYNTAX

[**no**] **interface vlan** *vlan-id*

*vlan-id* - ID of the configured VLAN. (Range: 1-4093, no leading zeroes)

#### DEFAULT SETTING
None

#### COMMAND MODE
Global Configuration

#### COMMAND USAGE
- Creating a "normal" VLAN with the vlan command initializes it as a Layer 2 interface. To change it to a Layer 3 interface, use the interface command to enter interface configuration for the desired VLAN, enter any Layer 3 configuration commands, and save the configuration settings.
- To change a Layer 3 normal VLAN back to a Layer 2 VLAN, use the no interface command.

#### EXAMPLE
The following example shows how to set the interface configuration mode to VLAN 1, and then assign an IP address to the VLAN:

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

#### RELATED COMMANDS
shutdown (811)
interface (806)
vlan (891)

### switchport acceptable-frame-types

This command configures the acceptable frame types for a port. Use the **no** form to restore the default.

#### SYNTAX
**switchport acceptable-frame-types** {**all** | **tagged**}

**no switchport acceptable-frame-types**

**all** - The port accepts all frames, tagged or untagged.

**tagged** - The port only receives tagged frames.

#### DEFAULT SETTING
All frame types

#### COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

#### COMMAND USAGE

When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN.

#### EXAMPLE

The following example shows how to restrict the traffic received on port 1 to tagged frames:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

#### RELATED COMMANDS

switchport mode (896)

### 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: 1-4093).

#### DEFAULT SETTING

All ports are assigned to VLAN 1 by default.
The default frame type is untagged.

#### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

#### COMMAND USAGE

- A port, or a trunk with switchport mode set to **hybrid**, must be assigned to at least one VLAN as untagged.
- If a trunk has switchport mode set to **trunk** (i.e., 1Q Trunk), then you can only assign an interface to VLAN groups as a tagged member.
- Frames are always tagged within the switch. The tagged/untagged parameter used when adding a VLAN to an interface tells the switch whether to keep or remove the tag from a frame on egress.
- If none of the intermediate network devices nor the host at the other end of the connection supports VLANs, the interface should be added to these VLANs as an

untagged member. Otherwise, it is only necessary to add at most one VLAN as untagged, and this should correspond to the native VLAN for the interface.

- If a VLAN on the forbidden list for an interface is manually added to that interface, the VLAN is automatically removed from the forbidden list for that interface.

### EXAMPLE

The following example shows how to add VLANs 1, 2, 5 and 6 to the allowed list as tagged VLANs for port 1:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 1,2,5,6 tagged
Console(config-if)#
```

## switchport ingress-filtering

This command enables ingress filtering for an interface. Use the **no** form to restore the default.

### SYNTAX

[**no**] **switchport ingress-filtering**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE

- Ingress filtering only affects tagged frames.
- If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).
- If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
- Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STA. However, they do affect VLAN dependent BPDU frames, such as GMRP.

### EXAMPLE

The following example shows how to set the interface to port 1 and then enable ingress filtering:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

## switchport mode

This command configures the VLAN membership mode for a port. Use the **no** form to restore the default.

### SYNTAX

**switchport mode** {**hybrid** | **trunk** | **private-vlan**}

**no switchport mode**

**hybrid** - Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.

**trunk** - Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. Note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are also transmitted as tagged frames.

**private-vlan** - For an explanation of this command see the switchport mode private-vlan command.

### DEFAULT SETTING

All ports are in 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)#
```

### RELATED COMMANDS

switchport acceptable-frame-types (893)

## 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: 1-4093, 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)#
```

## vlan-trunking

This command allows unknown VLAN groups to pass through the specified interface. Use the **no** form to disable this feature.

### SYNTAX

[**no**] **vlan-trunking**

### DEFAULT SETTING

Disabled

### COMMAND MODE

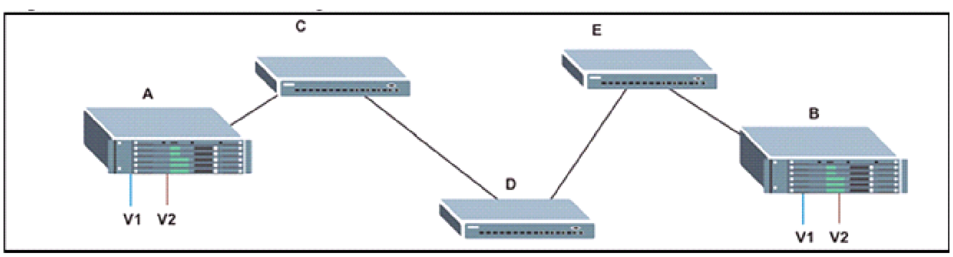
Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE

- Use this command to configure a tunnel across one or more intermediate switches which pass traffic for VLAN groups to which they do not belong.

  The following figure shows VLANs 1 and 2 configured on switches A and B, with VLAN trunking being used to pass traffic for these VLAN groups across switches C, D and E.

**Figure 1: Configuring VLAN Trunking**




Without VLAN trunking, you would have to configure VLANs 1 and 2 on all intermediate switches – C, D and E; otherwise these switches would drop any frames with unknown VLAN group tags. However, by enabling VLAN trunking on the intermediate switch ports along the path connecting VLANs 1 and 2, you only need to create these VLAN groups in switches A and B. Switches C, D and E automatically allow frames with VLAN group tags 1 and 2 (groups that are unknown to those switches) to pass through their VLAN trunking ports.

- VLAN trunking is mutually exclusive with the “access” switchport mode (see the switchport mode command). If VLAN trunking is enabled on an interface, then that interface cannot be set to access mode, and vice versa.
- To prevent loops from forming in the spanning tree, all unknown VLANs will be bound to a single instance (either STP/RSTP or an MSTP instance, depending on the selected STA mode).
- If both VLAN trunking and ingress filtering are disabled on an interface, packets with unknown VLAN tags will still be allowed to enter this interface and will be flooded to all other ports where VLAN trunking is enabled. (In other words, VLAN trunking will still be effectively enabled for the unknown VLAN).

#### Example

The following example enables VLAN trunking on ports 25 and 26 to establish a path across the switch for unknown VLAN groups:

```
Console(config)#interface ethernet 1/25
Console(config-if)#vlan-trunking
Console(config-if)#interface ethernet 1/26
Console(config-if)#vlan-trunking
Console(config-if)#
```

## Displaying VLAN Information

This section describes commands used to display VLAN information.

**Table 5: Commands for Displaying VLAN Information**

| Command | Function | Mode |
|---|---|---|
| show interfaces status vlan | Displays status for the specified VLAN interface | NE, PE |
| show interfaces switchport | Displays the administrative and operational status of an interface | NE, PE |
| show vlan | Shows VLAN information | NE, PE |

### show vlan

This command shows VLAN information.

#### Syntax

**show vlan** [**id** *vlan-id* | **name** *vlan-name* |
**private-vlan** *private-vlan-type*]

**id** - Keyword to be followed by the VLAN ID.

*vlan-id* - ID of the configured VLAN. (Range: 1-4093, no leading zeroes)

**name** - Keyword to be followed by the VLAN name.

*vlan-name* - ASCII string from 1 to 32 characters.

**private-vlan** - For an explanation of this command see the show vlan private-vlan command.

*private-vlan-type* - Indicates the private VLAN type.
(Options: community, primary)

### DEFAULT SETTING

Shows all VLANs.

### COMMAND MODE

Normal Exec, Privileged Exec

### EXAMPLE

The following example shows how to display information for VLAN 1:

```
Console#show vlan id 1

VLAN ID          : 1
Type             : Static
Name             : DefaultVlan
Status           : Active
Ports/Port Channels : Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
                      Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
                      Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S)
                      Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S) Eth1/20(S)
                      Eth1/21(S) Eth1/22(S) Eth1/23(S) Eth1/24(S) Eth1/25(S)
                      Eth1/26(S)
Console#
```

## CONFIGURING IEEE 802.1Q TUNNELING

IEEE 802.1Q tunneling (QinQ tunneling) uses a single Service Provider VLAN (SPVLAN) for customers who have multiple VLANs. Customer VLAN IDs are preserved and traffic from different customers is segregated within the service provider's network even when they use the same customer-specific VLAN IDs. QinQ tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy, preserving the customer's original tagged packets, and adding SPVLAN tags to each frame (also called double tagging).

This section describes commands used to configure QinQ tunneling.

**Table 6: 802.1Q Tunneling Commands**

| Command | Function | Mode |
|---|---|---|
| dot1q-tunnel system-tunnel-control | Configures the switch to operate in normal mode or QinQ mode | GC |
| switchport dot1q-tunnel mode | Configures an interface as a QinQ tunnel port | IC |
| switchport dot1q-tunnel service match cvid | Creates a CVLAN to SPVLAN mapping entry | IC |

**Table 6: 802.1Q Tunneling Commands**

| Command | Function | Mode |
|---|---|---|
| switchport dot1q-tunnel tpid | Sets the Tag Protocol Identifier (TPID) value of a tunnel port | IC |
| show dot1q-tunnel | Displays the configuration of QinQ tunnel ports | PE |
| show interfaces switchport | Displays port QinQ operational status | PE |

*General Configuration Guidelines for QinQ*

1. Configure the switch to QinQ mode (dot1q-tunnel system-tunnel-control).
2. Create a SPVLAN (vlan).
3. Configure the QinQ tunnel access port to dot1Q-tunnel access mode (switchport dot1q-tunnel mode).
4. Set the Tag Protocol Identifier (TPID) value of the tunnel access port. This step is required if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The standard ethertype value is 0x8100. (See switchport dot1q-tunnel tpid.)
5. Configure the QinQ tunnel access port to join the SPVLAN as an untagged member (switchport allowed vlan).
6. Configure the SPVLAN ID as the native VID on the QinQ tunnel access port (switchport native vlan).
7. Configure the QinQ tunnel uplink port to dot1Q-tunnel uplink mode (switchport dot1q-tunnel mode).
8. Configure the QinQ tunnel uplink port to join the SPVLAN as a tagged member (switchport allowed vlan).

*Limitations for QinQ*

- The native VLAN for the tunnel uplink ports and tunnel access ports cannot be the same. However, the same service VLANs can be set on both tunnel port types.
- IGMP Snooping should not be enabled on a tunnel access port.
- If the spanning tree protocol is enabled, be aware that a tunnel access or tunnel uplink port may be disabled if the spanning tree structure is automatically reconfigured to overcome a break in the tree. It is therefore advisable to disable spanning tree on these ports.

## dot1q-tunnel system-tunnel-control

This command sets the switch to operate in QinQ mode. Use the **no** form to disable QinQ operating mode.

### Syntax

[**no**] **dot1q-tunnel system-tunnel-control**

### DEFAULT SETTING
Disabled

### COMMAND MODE
Global Configuration

### COMMAND USAGE
QinQ tunnel mode must be enabled on the switch for QinQ interface settings to be functional.

### EXAMPLE

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#
```

### RELATED COMMANDS
show dot1q-tunnel (904)
show interfaces switchport (817)

## switchport dot1q-tunnel mode

This command configures an interface as a QinQ tunnel port. Use the **no** form to disable QinQ on the interface.

### SYNTAX

**switchport dot1q-tunnel mode** {**access** | **uplink**}

**no switchport dot1q-tunnel mode**

**access** – Sets the port as an 802.1Q tunnel access port.

**uplink** – Sets the port as an 802.1Q tunnel uplink port.

### DEFAULT SETTING
Disabled

### COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE
- QinQ tunneling must be enabled on the switch using the dot1q-tunnel system-tunnel-control command before the **switchport dot1q-tunnel mode** interface command can take effect.
- When a tunnel uplink port receives a packet from a customer, the customer tag (regardless of whether there are one or more tag layers) is retained in the inner tag, and the service provider’s tag added to the outer tag.
- When a tunnel uplink port receives a packet from the service provider, the outer service provider’s tag is stripped off, and the packet passed on to the VLAN indicated by the inner tag. If no inner tag is found, the packet is passed onto the native VLAN defined for the uplink port.

#### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#
```

#### RELATED COMMANDS

show dot1q-tunnel (904)
show interfaces switchport (817)

### switchport dot1q-tunnel service match cvid

This command creates a CVLAN to SPVLAN mapping entry. Use the **no** form to delete a VLAN mapping entry.

#### SYNTAX

**switchport dot1q-tunnel service** *svid* **match cvid** *cvid* [**remove-ctag**]

*svid* - VLAN ID for the outer VLAN tag (Service Provider VID). (Range: 1-4094, no leading zeroes)

*cvid* - VLAN ID for the inner VLAN tag (Customer VID). (Range: 1-4094, no leading zeroes)

**remove-ctag** - Removes the customer's VLAN tag.

#### DEFAULT SETTING

Default mapping uses the PVID of the ingress port on the edge router for the SPVID.

#### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

#### COMMAND USAGE

- The inner VLAN tag of a customer packet entering the edge router of a service provider's network is mapped to an outer tag indicating the service provider VLAN that will carry this traffic across the 802.1Q tunnel. By default, the outer tag is based on the default VID of the edge router's ingress port. This process is performed in a transparent manner as described under IEEE 802.1Q Tunneling.

- When priority bits are found in the inner tag, these are also copied to the outer tag. This allows the service provider to differentiate service based on the indicated priority and appropriate methods of queue management at intermediate nodes across the tunnel.

- Rather than relying on standard service paths and priority queuing, QinQ VLAN mapping can be used to further enhance service by defining a set of differentiated service pathways to follow across the service provider's network for traffic arriving from specified inbound customer VLANs.

- Note that all interfaces are configured as access interfaces by default (that is, a user-to-network interface). Using the switchport dot1q-tunnel mode uplink command configures an interface as an uplink interface (that is, a network-to-network interface).

- When the **remove-ctag** option is specified, the inner-tag containing the customer's VID is removed, and the outer-tag containing the service provider's VID remains in place.

### EXAMPLE

This example sets the SVID to 99 in the outer tag for egress packets exiting port 1 when the packet's CVID is 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel service 99 match cvid 2
Console(config-if)#
```

In the following examples, ports 1 and 2 are configured as follows:

Port 1 = Access, PVID = 100, VLAN = 100(u), 101(u)
Port 2 = Uplink, VLAN = 100(t), 101(t)

1. Inject tagged frame (VID=10) to Port 1, then
=> Port 2: exits double-tagged frame (SVID=100, CVID=10)
(*switching*)

2. Port 1: switchport dot1q-tunnel service 101 match cvid 10
Inject tagged frame (VID=10) to Port 1, then
=> Port 2: exits double-tagged frame (SVID=101, CVID=10)
(*ingress vlan translation*)

Inject double-tagged frame (SVID=101, CVID=10) to Port 2, then
=> Port 1: exits single-tagged frame (VID=10)
(*switching*)

3. Port 1: switchport dot1q-tunnel service 101 match cvid 10 remove-ctag
Inject tagged frame (VID=10) to Port 1, then
=> Port 2: exits single-tagged frame (SVID=101)
(*ingress vlan translation*)

Inject single-tagged frame (SVID=101) to Port 2, then
=> Port 1: exits single-tagged frame (VID=10)
(*egress vlan translation*)

## switchport dot1q-tunnel tpid

This command sets the Tag Protocol Identifier (TPID) value of a tunnel port. Use the **no** form to restore the default setting.

### SYNTAX

**switchport dot1q-tunnel tpid** *tpid*

**no switchport dot1q-tunnel tpid**

*tpid* – Sets the ethertype value for 802.1Q encapsulation. This identifier is used to select a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The standard ethertype value is 0x8100. (Range: 0800-FFFF hexadecimal)

#### Default Setting

0x8100

#### Command Mode

Interface Configuration (Ethernet, Port Channel)

#### Command Usage

- Use the **switchport dot1q-tunnel tpid** command to set a custom 802.1Q ethertype value on the selected interface. This feature allows the switch to interoperate with third-party switches that do not use the standard 0x8100 ethertype to identify 802.1Q-tagged frames. For example, 0x1234 is set as the custom 802.1Q ethertype on a trunk port, incoming frames containing that ethertype are assigned to the VLAN contained in the tag following the ethertype field, as they would be with a standard 802.1Q trunk. Frames arriving on the port containing any other ethertype are looked upon as untagged frames, and assigned to the native VLAN of that port.

- All ports on the switch will be set to the same ethertype.

#### Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel tpid 9100
Console(config-if)#
```

#### Related Commands

show interfaces switchport (817)

### show dot1q-tunnel

This command displays information about QinQ tunnel ports.

#### Syntax

**show dot1q-tunnel** [**interface** *interface* [**service** *svid*] | **service** [*svid*]]

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

*svid* - VLAN ID for the outer VLAN tag (SPVID). (Range: 1-4094, no leading zeroes)

#### Command Mode

Privileged Exec

#### Example

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#interface ethernet 1/2
Console(config-if)#switchport dot1q-tunnel mode uplink
```

```
Console(config-if)#end
Console#show dot1q-tunnel

Current double-tagged status of the system is Enabled
The dot1q-tunnel mode of the set interface 1/1 is Access mode, TPID is 0x8100.
The dot1q-tunnel mode of the set interface 1/2 is Uplink mode, TPID is 0x8100.
The dot1q-tunnel mode of the set interface 1/3 is Normal mode, TPID is 0x8100.
:
Console#show dot1q-tunnel interface ethernet 1/5
802.1Q Tunnel Service Subscriptions

 Port     Match C-VID S-VID Remove C-Tag
 -------- ----------- ----- ------------
 Eth 1/ 5           1   100 Disabled

Console#show dot1q-tunnel service 100
802.1Q Tunnel Service Subscriptions

 Port     Match C-VID S-VID Remove C-Tag
 -------- ----------- ----- ------------
 Eth 1/ 5           1   100 Disabled
 Eth 1/ 6           1   100 Enabled

Console#
```

### RELATED COMMANDS

switchport dot1q-tunnel mode (901)

## CONFIGURING PORT-BASED TRAFFIC SEGMENTATION

If tighter security is required for passing traffic from different clients through downlink ports on the local network and over uplink ports to the service provider, port-based traffic segmentation can be used to isolate traffic for individual clients.

**Table 7: Commands for Configuring Traffic Segmentation**

| Command | Function | Mode |
|---|---|---|
| traffic-segmentation | Enables and configures traffic segmentation | GC |
| show traffic-segmentation | Displays the configured traffic segments | PE |

### traffic-segmentation

This command enables traffic segmentation globally, or configures the uplink and down-link ports for a segmented group of ports. Use the **no** form to disable traffic segmentation globally.

#### SYNTAX

[**no**] **traffic-segmentation** [**uplink** *interface-list* **downlink** *interface-list*]

**uplink** – Specifies an uplink interface.

**downlink** – Specifies a downlink interface.

#### Default Setting

Disabled globally

No segmented port groups are defined.

#### Command Mode

Global Configuration

#### Command Usage

- Traffic segmentation provides port-based security and isolation between ports within the VLAN. Data traffic on the downlink ports can only be forwarded to, and from, the designated uplink port(s). Data cannot pass between downlink ports in the same segmented group, nor to ports which do not belong to the same group.
- Any port can be defined as an uplink port or downlink port, but cannot be configured to serve both roles.
- Traffic segmentation and normal VLANs can exist simultaneously within the same switch. Traffic may pass freely between uplink ports in segmented groups and ports in normal VLANs.
- Enter the **traffic-segmentation** command without any parameters to enable traffic segmentation. Then set the interface members for segmented groups.
- Enter **no traffic-segmentation** to disable traffic segmentation and clear the configuration settings for segmented groups.

#### Example

This example enables traffic segmentation, and then sets port 12 as the uplink and ports 5-8 as downlinks.

```
Console(config)#traffic-segmentation
Console(config)#traffic-segmentation uplink ethernet 1/12 downlink ethernet 1/5-8
Console(config)#
```

## show traffic-segmentation

This command displays the configured traffic segments.

#### Command Mode

Privileged Exec

#### Example

```
Console#show traffic-segmentation
Private VLAN status: Disabled
Up-link Port:
 Ethernet 1/12
Down-link Port:
 Ethernet 1/5
 Ethernet 1/6
 Ethernet 1/7
 Ethernet 1/8
Console#
```

## CONFIGURING PRIVATE VLANS

Private VLANs provide port-based security and isolation of local ports contained within different private VLAN groups. This switch supports two types of private VLANs – primary and community groups. A primary VLAN contains promiscuous ports that can communicate with all other ports in the associated private VLAN groups, while a community (or secondary) VLAN contains community ports that can only communicate with other hosts within the community VLAN and with any of the promiscuous ports in the associated primary VLAN. The promiscuous ports are designed to provide open access to an external network such as the Internet, while the community ports provide restricted access to local users.

Multiple primary VLANs can be configured on this switch, and multiple community VLANs can be associated with each primary VLAN. (Note that private VLANs and normal VLANs can exist simultaneously within the same switch.)

This section describes commands used to configure private VLANs.

**Table 8: Private VLAN Commands**

| Command | Function | Mode |
|---|---|---|
| *Edit Private VLAN Groups* | | |
| private-vlan | Adds or deletes primary or community VLANs | VC |
| private vlan association | Associates a community VLAN with a primary VLAN | VC |
| *Configure Private VLAN Interfaces* | | |
| switchport mode private-vlan | Sets an interface to host mode or promiscuous mode | IC |
| switchport private-vlan host-association | Associates an interface with a secondary VLAN | IC |
| switchport private-vlan mapping | Maps an interface to a primary VLAN | IC |
| *Display Private VLAN Information* | | |
| show vlan private-vlan | Shows private VLAN information | NE, PE |

To configure private VLANs, follow these steps:

1. Use the private-vlan command to designate one or more community VLANs and the primary VLAN that will channel traffic outside of the community groups.

2. Use the private vlan association command to map the community VLAN(s) to the primary VLAN.

3. Use the switchport mode private-vlan command to configure ports as promiscuous (i.e., having access to all ports in the primary VLAN) or host (i.e., community port).

4. Use the switchport private-vlan host-association command to assign a port to a community VLAN.

5. Use the switchport private-vlan mapping command to assign a port to a primary VLAN.

6. Use the show vlan private-vlan command to verify your configuration settings.

## private-vlan

Use this command to create a primary or community private VLAN. Use the **no** form to remove the specified private VLAN.

### Syntax

**private-vlan** *vlan-id* {**community** | **primary**}

**no private-vlan** *vlan-id*

*vlan-id* - ID of private VLAN. (Range: 1-4093, no leading zeroes).

**community** - A VLAN in which traffic is restricted to host members in the same VLAN and to promiscuous ports in the associate primary VLAN.

**primary** - A VLAN which can contain one or more community VLANs, and serves to channel traffic between community VLANs and other locations.

### Default Setting

None

### Command Mode

VLAN Configuration

### Command Usage

- Private VLANs are used to restrict traffic to ports within the same community, and channel traffic passing outside the community through promiscuous ports. When using community VLANs, they must be mapped to an associated “primary” VLAN that contains promiscuous ports.

- Port membership for private VLANs is static. Once a port has been assigned to a private VLAN, it cannot be dynamically moved to another VLAN via GVRP.

- Private VLAN ports cannot be set to trunked mode. (See switchport mode)

### Example

```
Console(config)#vlan database
Console(config-vlan)#private-vlan 2 primary
Console(config-vlan)#private-vlan 3 community
Console(config)#
```

## private vlan association

Use this command to associate a primary VLAN with a secondary (i.e., community) VLAN. Use the **no** form to remove all associations for the specified primary VLAN.

### SYNTAX

**private-vlan** *primary-vlan-id* **association** {*secondary-vlan-id* **| add** *secondary-vlan-id* | **remove** *secondary-vlan-id*}

**no private-vlan** *primary-vlan-id* **association**

*primary-vlan-id* - ID of primary VLAN. (Range: 1-4093, no leading zeroes).

*secondary-vlan-id* - ID of secondary (i.e, community) VLAN. (Range: 1-4093, no leading zeroes).

### DEFAULT SETTING

None

### COMMAND MODE

VLAN Configuration

### COMMAND USAGE

Secondary VLANs provide security for group members. The associated primary VLAN provides a common interface for access to other network resources within the primary VLAN (e.g., servers configured with promiscuous ports) and to resources outside of the primary VLAN (via promiscuous ports).

### EXAMPLE

```
Console(config-vlan)#private-vlan 2 association 3
Console(config)#
```

## switchport mode private-vlan

Use this command to set the private VLAN mode for an interface. Use the **no** form to restore the default setting.

### SYNTAX

**switchport mode private-vlan** {**host** | **promiscuous**}

**no switchport mode private-vlan**

**host** – This port type can subsequently be assigned to a community VLAN.

**promiscuous** – This port type can communicate with all other promiscuous ports in the same primary VLAN, as well as with all the ports in the associated secondary VLANs.

### DEFAULT SETTING

Normal VLAN

### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE

To assign a promiscuous port to a primary VLAN, use the switchport private-vlan mapping command. To assign a host port to a community VLAN, use the switchport private-vlan host-association command.

### EXAMPLE

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport mode private-vlan promiscuous
Console(config-if)#exit
Console(config)#interface ethernet 1/3
Console(config-if)#switchport mode private-vlan host
Console(config-if)#
```

## switchport private-vlan host-association

Use this command to associate an interface with a secondary VLAN. Use the **no** form to remove this association.

### SYNTAX

**switchport private-vlan host-association** *secondary-vlan-id*

**no switchport private-vlan host-association**

*secondary-vlan-id* - ID of secondary (i.e., community) VLAN. (Range: 1-4093, no leading zeroes).

### DEFAULT SETTING

None

### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE

All ports assigned to a secondary (i.e., community) VLAN can pass traffic between group members, but must communicate with resources outside of the group via promiscuous ports in the associated primary VLAN.

### EXAMPLE

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport private-vlan host-association 3
Console(config-if)#
```

## switchport private-vlan mapping

Use this command to map an interface to a primary VLAN. Use the **no** form to remove this mapping.

### SYNTAX

**switchport private-vlan mapping** *primary-vlan-id*

**no switchport private-vlan mapping**

*primary-vlan-id* – ID of primary VLAN. (Range: 1-4093, no leading zeroes).

#### DEFAULT SETTING
None

#### COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

#### COMMAND USAGE
Promiscuous ports assigned to a primary VLAN can communicate with any other promiscuous ports in the same VLAN, and with the group members within any associated secondary VLANs.

#### EXAMPLE

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport private-vlan mapping 2
Console(config-if)#
```

### show vlan private-vlan

Use this command to show the private VLAN configuration settings on this switch.

#### SYNTAX

**show vlan private-vlan** [**community** | **primary**]

**community** – Displays all community VLANs, along with their associated primary VLAN and assigned host interfaces.

**primary** – Displays all primary VLANs, along with any assigned promiscuous interfaces.

#### DEFAULT SETTING
None

#### COMMAND MODE
Privileged Executive

#### EXAMPLE

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

## CONFIGURING PROTOCOL-BASED VLANS

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type in use by the inbound packets.

.
**Table 9: Protocol-based VLAN Commands**

| Command | Function | Mode |
|---|---|---|
| protocol-vlan protocol-group | Create a protocol group, specifying the supported protocols | GC |
| protocol-vlan protocol-group | Maps a protocol group to a VLAN | IC |
| show protocol-vlan protocol-group | Shows the configuration of protocol groups | PE |
| show interfaces protocol-vlan protocol-group | Shows the interfaces mapped to a protocol group and the corresponding VLAN | PE |

To configure protocol-based VLANs, follow these steps:

1. First configure VLAN groups for the protocols you want to use (page 891). Although not mandatory, we suggest configuring a separate VLAN for each major protocol running on your network. Do not add port members at this time.
2. Create a protocol group for each of the protocols you want to assign to a VLAN using the protocol-vlan protocol-group command (Global Configuration mode).
3. Then map the protocol for each interface to the appropriate VLAN using the protocol-vlan protocol-group command (Interface Configuration mode).

### protocol-vlan protocol-group (Configuring Groups)

This command creates a protocol group, or to add specific protocols to a group. Use the **no** form to remove a protocol group.

#### SYNTAX

**protocol-vlan protocol-group** *group-id* [{**add** | **remove**} **frame-type** *frame* **protocol-type** *protocol*]

**no protocol-vlan protocol-group** *group-id*

*group-id* - Group identifier of this protocol group. (Range: 1-2147483647)

*frame*[1] - Frame type used by this protocol. (Options: ethernet, rfc_1042, llc_other)

1. SNAP frame types are not supported by this switch due to hardware limitations.

*protocol* - Protocol type. The only option for the llc_other frame type is ipx_raw. The options for all other frames types include: arp, ip, ipv6, rarp.

**DEFAULT SETTING**
No protocol groups are configured.

**COMMAND MODE**
Global Configuration

**EXAMPLE**
The following creates protocol group 1, and specifies Ethernet frames with IP and ARP protocol types:

```
Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet protocol-type ip
Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet protocol-type arp
Console(config)#
```

## protocol-vlan protocol-group (Configuring Interfaces)

This command maps a protocol group to a VLAN for the current interface. Use the **no** form to remove the protocol mapping for this interface.

**SYNTAX**

**protocol-vlan protocol-group** *group-id* **vlan** *vlan-id*

**no protocol-vlan protocol-group** *group-id* **vlan**

*group-id* - Group identifier of this protocol group. (Range: 1-2147483647)

*vlan-id* - VLAN to which matching protocol traffic is forwarded. (Range: 1-4093)

**DEFAULT SETTING**
No protocol groups are mapped for any interface.

**COMMAND MODE**
Interface Configuration (Ethernet, Port Channel)

**COMMAND USAGE**

- When creating a protocol-based VLAN, only assign interfaces via this command. If you assign interfaces using any of the other VLAN commands (such as the vlan command), these interfaces will admit traffic of any protocol type into the associated VLAN.

- When a frame enters a port that has been assigned to a protocol VLAN, it is processed in the following manner:

  - If the frame is tagged, it will be processed according to the standard rules applied to tagged frames.

  - If the frame is untagged and the protocol type matches, the frame is forwarded to the appropriate VLAN.

- If the frame is untagged but the protocol type does not match, the frame is forwarded to the default VLAN for this interface.

**EXAMPLE**

The following example maps the traffic entering Port 1 which matches the protocol type specified in protocol group 1 to VLAN 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan 2
Console(config-if)#
```

## show protocol-vlan protocol-group

This command shows the frame and protocol type associated with protocol groups.

**SYNTAX**

**show protocol-vlan protocol-group** [*group-id*]

*group-id* - Group identifier for a protocol group. (Range: 1-2147483647)

**DEFAULT SETTING**

All protocol groups are displayed.

**COMMAND MODE**

Privileged Exec

**EXAMPLE**

This shows protocol group 1 configured for IP over Ethernet:

```
Console#show protocol-vlan protocol-group

 Protocol Group ID  Frame Type   Protocol Type
------------------ ------------- ---------------
                1      ethernet     08 00
Console#
```

## show interfaces protocol-vlan protocol-group

This command shows the mapping from protocol groups to VLANs for the selected interfaces.

**SYNTAX**

**show interfaces protocol-vlan protocol-group** [*interface*]

*interface*

**ethernet** *unit/port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-12)

### DEFAULT SETTING

The mapping for all interfaces is displayed.

### COMMAND MODE

Privileged Exec

### EXAMPLE

This shows that traffic entering Port 1 that matches the specifications for protocol group 1 will be mapped to VLAN 2:

```
Console#show interfaces protocol-vlan protocol-group

  Port     ProtocolGroup ID    VLAN ID
---------- ------------------ -----------
  Eth 1/1                 1       vlan2
Console#
```

## CONFIGURING IP SUBNET VLANS

When using IEEE 802.1Q port-based VLAN classification, all untagged frames received by a port are classified as belonging to the VLAN whose VID (PVID) is associated with that port.

When IP subnet-based VLAN classification is enabled, the source address of untagged ingress frames are checked against the IP subnet-to-VLAN mapping table. If an entry is found for that subnet, these frames are assigned to the VLAN indicated in the entry. If no IP subnet is matched, the untagged frames are classified as belonging to the receiving port's VLAN ID (PVID).

**Table 10: IP Subnet VLAN Commands**

| Command | Function | Mode |
|---|---|---|
| subnet-vlan | Defines the IP Subnet VLANs | GC |
| show subnet-vlan | Displays IP Subnet VLAN settings | PE |

## subnet-vlan

This command configures IP Subnet VLAN assignments. Use the **no** form to remove an IP subnet-to-VLAN assignment.

### SYNTAX

**subnet-vlan subnet** *ip-address mask* **vlan** *vlan-id* [**priority** *priority*]

**no subnet-vlan subnet** {*ip-address mask* | **all**}

*ip-address* – The IP address that defines the subnet. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.

*mask* – This mask identifies the host address bits of the IP subnet.

*vlan-id* – VLAN to which matching IP subnet traffic is forwarded. (Range: 1-4093)

*priority* – The priority assigned to untagged ingress traffic. (Range: 0-7, where 7 is the highest priority)

### DEFAULT SETTING

Priority: 0

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- Each IP subnet can be mapped to only one VLAN ID. An IP subnet consists of an IP address and a subnet mask.
- When an untagged frame is received by a port, the source IP address is checked against the IP subnet-to-VLAN mapping table, and if an entry is found, the corresponding VLAN ID is assigned to the frame. If no mapping is found, the PVID of the receiving port is assigned to the frame.
- The IP subnet cannot be a broadcast or multicast IP address.
- When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

### EXAMPLE

The following example assigns traffic for the subnet 192.168.12.192, mask 255.255.255.224, to VLAN 4.

```
Console(config)#subnet-vlan subnet 192.168.12.192 255.255.255.224 vlan 4
Console(config)#
```

## show subnet-vlan

This command displays IP Subnet VLAN assignments.

### COMMAND MODE

Privileged Exec

### COMMAND USAGE

- Use this command to display subnet-to-VLAN mappings.
- The last matched entry is used if more than one entry can be matched.

### EXAMPLE

The following example displays all configured IP subnet-based VLANs.

```
Console#show subnet-vlan
IP Address        Mask             VLAN ID  Priority
---------------  ---------------  -------  --------
192.168.12.0     255.255.255.128     1        0
192.168.12.128   255.255.255.192     3        0
192.168.12.192   255.255.255.224     4        0
192.168.12.224   255.255.255.240     5        0
192.168.12.240   255.255.255.248     6        0
192.168.12.248   255.255.255.252     7        0
192.168.12.252   255.255.255.254     8        0
192.168.12.254   255.255.255.255     9        0
192.168.12.255   255.255.255.255    10        0
Console#
```

## CONFIGURING MAC BASED VLANS

When using IEEE 802.1Q port-based VLAN classification, all untagged frames received by a port are classified as belonging to the VLAN whose VID (PVID) is associated with that port.

When MAC-based VLAN classification is enabled, the source address of untagged ingress frames are checked against the MAC address-to-VLAN mapping table. If an entry is found for that address, these frames are assigned to the VLAN indicated in the entry. If no MAC address is matched, the untagged frames are classified as belonging to the receiving port's VLAN ID (PVID).

**Table 11: MAC Based VLAN Commands**

| Command | Function | Mode |
|---|---|---|
| mac-vlan | Defines the IP Subnet VLANs | GC |
| show mac-vlan | Displays IP Subnet VLAN settings | PE |

### mac-vlan

This command configures MAC address-to-VLAN mapping. Use the **no** form to remove an assignment.

### SYNTAX

**mac-vlan mac-address** *mac-address* **vlan** *vlan-id* [**priority** *priority*]

**no mac-vlan mac-address** {*mac-address* | **all**} *mac-address* – The source MAC address to be matched. Configured MAC addresses can only be unicast addresses. The MAC address must be specified in the format xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.

*vlan-id* – VLAN to which the matching source MAC address traffic is forwarded. (Range: 1-4093)

*priority* – The priority assigned to untagged ingress traffic. (Range: 0-7, where 7 is the highest priority)

#### DEFAULT SETTING
None

#### COMMAND MODE
Global Configuration

#### COMMAND USAGE
- The MAC-to-VLAN mapping applies to all ports on the switch.
- Source MAC addresses can be mapped to only one VLAN ID.
- Configured MAC addresses cannot be broadcast or multicast addresses.
- When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

#### EXAMPLE
The following example assigns traffic from source MAC address 00-00-00-11-22-33 to VLAN 10.

```
Console(config)#mac-vlan mac-address 00-00-00-11-22-33 vlan 10
Console(config)#
```

### show mac-vlan

This command displays MAC address-to-VLAN assignments.

#### COMMAND MODE
Privileged Exec

#### COMMAND USAGE
Use this command to display MAC address-to-VLAN mappings.

#### EXAMPLE
The following example displays all configured MAC address-based VLANs.

```
Console#show mac-vlan
MAC Address        VLAN ID   Priority
-----------------  --------  --------
00-00-00-11-22-33       10         0
Console#
```

## CONFIGURING VOICE VLANS

The switch allows you to specify a Voice VLAN for the network and set a CoS priority for the VoIP traffic. VoIP traffic can be detected on switch ports by using the source MAC address of packets, or by using LLDP (IEEE 802.1AB) to discover connected VoIP devices. When VoIP traffic is detected on a configured port, the switch automatically assigns the port to the Voice VLAN. Alternatively, switch ports can be manually configured.

**Table 12: Voice VLAN Commands**

| Command | Function | Mode |
|---|---|---|
| voice vlan | Defines the Voice VLAN ID | GC |
| voice vlan aging | Configures the aging time for Voice VLAN ports | GC |
| voice vlan mac-address | Configures VoIP device MAC addresses | GC |
| switchport voice vlan | Sets the Voice VLAN port mode | IC |
| switchport voice vlan priority | Sets the VoIP traffic priority for ports | IC |
| switchport voice vlan rule | Sets the automatic VoIP traffic detection method for ports | IC |
| switchport voice vlan security | Enables Voice VLAN security on ports | IC |
| show voice vlan | Displays Voice VLAN settings | PE |

### voice vlan

This command enables VoIP traffic detection and defines the Voice VLAN ID. Use the **no** form to disable the Voice VLAN.

#### SYNTAX

**voice vlan** *voice-vlan-id*

**no voice vlan**

*voice-vlan-id* - Specifies the voice VLAN ID. (Range: 1-4093)

#### DEFAULT SETTING

Disabled

#### COMMAND MODE

Global Configuration

#### COMMAND USAGE

- When IP telephony is deployed in an enterprise network, it is recommended to isolate the Voice over IP (VoIP) network traffic from other data traffic. Traffic isolation helps prevent excessive packet delays, packet loss, and jitter, which results in higher voice quality. This is best achieved by assigning all VoIP traffic to a single VLAN.

- VoIP traffic can be detected on switch ports by using the source MAC address of packets, or by using LLDP (IEEE 802.1AB) to discover connected VoIP devices. When VoIP traffic is detected on a configured port, the switch automatically assigns the port as a tagged member of the Voice VLAN.

- Only one Voice VLAN is supported and it must already be created on the switch before it can be specified as the Voice VLAN.
- The Voice VLAN ID cannot be modified when the global auto-detection status is enabled (see the switchport voice vlan command.

**EXAMPLE**

The following example enables VoIP traffic detection and specifies the Voice VLAN ID as 1234.

```
Console(config)#voice vlan 1234
Console(config)#
```

## voice vlan aging

This command sets the Voice VLAN ID time out. Use the **no** form to restore the default.

**SYNTAX**

**voice vlan aging** *minutes*

**no voice vlan**

*minutes* - Specifies the port Voice VLAN membership time out. (Range: 5-43200 minutes)

**DEFAULT SETTING**

1440 minutes

**COMMAND MODE**

Global Configuration

**COMMAND USAGE**

The Voice VLAN aging time is the time after which a port is removed from the Voice VLAN when VoIP traffic is no longer received on the port.

**EXAMPLE**

The following example configures the Voice VLAN aging time as 3000 minutes.

```
Console(config)#voice vlan aging 3000
Console(config)#
```

## voice vlan mac-address

This command specifies MAC address ranges to add to the OUI Telephony list. Use the **no** form to remove an entry from the list.

### Syntax

**voice vlan mac-address** *mac-address* **mask** *mask-address* [**description** *description*]

**no voice vlan mac-address** *mac-address* **mask** *mask-address*

*mac-address* - Defines a MAC address OUI that identifies VoIP devices in the network. (For example, 01-23-45-00-00-00)

*mask-address* - Identifies a range of MAC addresses. (Range: 80-00-00-00-00-00 to FF-FF-FF-FF-FF-FF)

*description* - User-defined text that identifies the VoIP devices. (Range: 1-32 characters)

### Default Setting

None

### Command Mode

Global Configuration

### Command Usage

- VoIP devices attached to the switch can be identified by the manufacturer's Organizational Unique Identifier (OUI) in the source MAC address of received packets. OUI numbers are assigned to manufacturers and form the first three octets of device MAC addresses. The MAC OUI numbers for VoIP equipment can be configured on the switch so that traffic from these devices is recognized as VoIP.

- Selecting a mask of FF-FF-FF-00-00-00 identifies all devices with the same OUI (the first three octets). Other masks restrict the MAC address range. Selecting FF-FF-FF-FF-FF-FF specifies a single MAC address.

### Example

The following example adds a MAC OUI to the OUI Telephony list.

```
Console(config)#voice vlan mac-address 00-12-34-56-78-90 mask ff-ff-ff-00-00-00 description A new
  phone
Console(config)#
```

## switchport voice vlan

This command specifies the Voice VLAN mode for ports. Use the **no** form to disable the Voice VLAN feature on the port.

### Syntax

**switchport voice vlan** {**manual** | **auto**}

**no switchport voice vlan**

**manual** - The Voice VLAN feature is enabled on the port, but the port must be manually added to the Voice VLAN.

**auto** - The port will be added as a tagged member to the Voice VLAN when VoIP traffic is detected on the port.

### Default Setting

Disabled

### Command Mode

Interface Configuration

### Command Usage

When auto is selected, you must select the method to use for detecting VoIP traffic, either OUI or 802.1ab (LLDP) using the switchport voice vlan rule command. When OUI is selected, be sure to configure the MAC address ranges in the Telephony OUI list using the voice vlan mac-address command.

### Example

The following example sets port 1 to Voice VLAN auto mode.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan auto
Console(config-if)#
```

## switchport voice vlan priority

This command specifies a CoS priority for VoIP traffic on a port. Use the **no** form to restore the default priority on a port.

### Syntax

**switchport voice vlan priority** *priority-value*

**no switchport voice vlan priority**

*priority-value* - The CoS priority value. (Range: 0-6)

### Default Setting

6

### Command Mode

Interface Configuration

### COMMAND USAGE

Specifies a CoS priority to apply to the port VoIP traffic on the Voice VLAN. The priority of any received VoIP packet is overwritten with the new priority when the Voice VLAN feature is active for the port.

### EXAMPLE

The following example sets the CoS priority to 5 on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan priority 5
Console(config-if)#
```

## switchport voice vlan rule

This command selects a method for detecting VoIP traffic on a port. Use the **no** form to disable the detection method on the port.

### SYNTAX

[**no**] **switchport voice vlan rule** {**oui** | **lldp**}

**oui** - Traffic from VoIP devices is detected by the Organizationally Unique Identifier (OUI) of the source MAC address.

**lldp** - Uses LLDP to discover VoIP devices attached to the port.

### DEFAULT SETTING

OUI: Enabled
LLDP: Disabled

### COMMAND MODE

Interface Configuration

### COMMAND USAGE

- When OUI is selected, be sure to configure the MAC address ranges in the Telephony OUI list (see the voice vlan mac-address command. MAC address OUI numbers must be configured in the Telephony OUI list so that the switch recognizes the traffic as being from a VoIP device.

- LLDP checks that the “telephone bit” in the system capability TLV is turned on. See LLDP Commands for more information on LLDP.

### EXAMPLE

The following example enables the OUI method on port 1 for detecting VoIP traffic.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan rule oui
Console(config-if)#
```

## switchport voice vlan security

This command enables security filtering for VoIP traffic on a port. Use the **no** form to disable filtering on a port.

#### Syntax

**[no] switchport voice vlan security**

#### Default Setting

Disabled

#### Command Mode

Interface Configuration

#### Command Usage

- Security filtering discards any non-VoIP packets received on the port that are tagged with the voice VLAN ID. VoIP traffic is identified by source MAC addresses configured in the Telephony OUI list, or through LLDP that discovers VoIP devices attached to the switch. Packets received from non-VoIP sources are dropped.
- When enabled, be sure the MAC address ranges for VoIP devices are configured in the Telephony OUI list (voice vlan mac-address).

#### Example

The following example enables security filtering on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan security
Console(config-if)#
```

### show voice vlan

This command displays the Voice VLAN settings on the switch and the OUI Telephony list.

#### Syntax

**show voice vlan** {**oui** | **status**}

**oui** - Displays the OUI Telephony list.

**status** - Displays the global and port Voice VLAN settings.

#### Default Setting

None

#### Command Mode

Privileged Exec

#### Example

```
Console#show voice vlan status
Global Voice VLAN Status
Voice VLAN Status     : Enabled
Voice VLAN ID         : 1234
Voice VLAN aging time : 1440 minutes

Voice VLAN Port Summary
Port    Mode    Security Rule    Priority Remaining Age
```

```
                                         (minutes)
-------- -------- -------- --------- -------- -------------
Eth 1/ 1 Auto     Enabled  OUI            6 100
Eth 1/ 2 Disabled Disabled OUI            6 NA
Eth 1/ 3 Manual   Enabled  OUI            5 100
Eth 1/ 4 Auto     Enabled  OUI            6 100
Eth 1/ 5 Disabled Disabled OUI            6 NA
Eth 1/ 6 Disabled Disabled OUI            6 NA
Eth 1/ 7 Disabled Disabled OUI            6 NA
Eth 1/ 8 Disabled Disabled OUI            6 NA
Eth 1/ 9 Disabled Disabled OUI            6 NA
Eth 1/10 Disabled Disabled OUI            6 NA

Console#show voice vlan oui
OUI Address       Mask              Description
----------------- ----------------- ------------------------------
00-12-34-56-78-9A FF-FF-FF-00-00-00 old phones
00-11-22-33-44-55 FF-FF-FF-00-00-00 new phones
00-98-76-54-32-10 FF-FF-FF-FF-FF-FF Chris' phone

Console#
```

# 40 CLASS OF SERVICE COMMANDS

The commands described in this section allow you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with eight priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. The default priority can be set for each interface, also the queue service mode and the mapping of frame priority tags to the switch's priority queues can be configured.

**Table 1: Priority Commands**

| Command Group | Function |
|---|---|
| Priority Commands (Layer 2) | Configures the queue mode, queue weights, and default priority for untagged frames |
| Priority Commands (Layer 3 and 4) | Maps TCP ports, IP precedence tags, or IP DSCP tags to class of service values |

## PRIORITY COMMANDS (LAYER 2)

This section describes commands used to configure Layer 2 traffic priority on the switch.

**Table 2: Priority Commands (Layer 2)**

| Command | Function | Mode |
|---|---|---|
| queue cos-map | Assigns class-of-service values to the priority queues | IC |
| queue mode | Sets the queue mode to strict priority, Weighted Round-Robin (WRR), or a combination of strict and weighted queuing | IC |
| queue weight | Assigns round-robin weights to the priority queues | IC |
| switchport priority default | Sets a port priority for incoming untagged frames | IC |
| show interfaces switchport | Displays the administrative and operational status of an interface | PE |
| show queue cos-map | Shows the class-of-service map | PE |
| show queue mode | Shows the current queue mode | PE |
| show queue weight | Shows weights assigned to the weighted queues | PE |

## queue cos-map

This command assigns class of service (CoS) values to the priority queues (i.e., hardware output queues 0 - 7). 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 7, where 7 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 eight priority queues, with Weighted Round Robin queuing for each port. Eight separate traffic classes are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown below.

**Table 3: Default CoS Priority Levels**

| **Priority** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| **Queue** | 2 | 0 | 1 | 3 | 4 | 5 | 6 | 7 |

### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE

- CoS values assigned at the ingress port are also used at the egress port.
- This command sets the CoS priority for all interfaces.

### EXAMPLE

The following example shows how to change the CoS assignments to a one-to-one mapping:

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

### RELATED COMMANDS

show queue cos-map (932)

## queue mode

This command sets the scheduling mode used for processing each of the class of service (CoS) priority queues. The options include strict priority, Weighted Round-Robin (WRR), or a combination of strict and weighted queuing. Use the **no** form to restore the default value.

### SYNTAX

**queue mode** {**strict** | **wrr** | **strict-wrr** [*queue-type-list*]}

**no queue mode**

**strict** - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues. This ensures that the highest priority packets are always serviced first, ahead of all other traffic.

**wrr** - Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights (based on the queue weight command), and servicing each queue in a round-robin fashion.

**strict-wrr** - Strict priority is used for the high-priority queues and Weighted Round-Robin for the rest of the queues.

*queue-type-list* - Indicates if the queue is a normal or strict type. (Options: 0 indicates a normal queue, 1 indicates a strict queue)

### DEFAULT SETTING

Weighted Round Robin

### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE

- The switch can be set to service the port queues based on strict priority, WRR, or a combination of strict and weighted queueing.
- Strict priority requires all traffic in a higher priority queue to be processed before lower priority queues are serviced.
- Weighted Round-Robin (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. Use the queue weight command to assign weights for WRR queuing to the eight priority queues.
- If Strict and WRR mode is selected, a combination of strict service is used for the high priority queues and weighted service for the remaining queues. The queues assigned to use strict priority should be specified using the Strict Mode field parameter.
- A weight can be assigned to each of the weighted queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue is polled for service, and subsequently affects the response time for software applications assigned a specific priority value.
- Service time is shared at the egress ports by defining scheduling weights for WRR, or for the queuing mode that uses a combination of strict and weighted

queuing. Service time is allocated to each queue by calculating a precise number of bytes per second that will be serviced on each round.

#### EXAMPLE

The following example sets the queue mode to strict priority service mode:

```
Console(config)#interface ge1/1
Console(config-if)#queue mode strict
Console(config-if)#
```

#### RELATED COMMANDS

queue weight (930)
show queue mode (932)

### queue weight

This command assigns weights to the eight class of service (CoS) priority queues when using weighted queuing, or one of the queuing modes that use a combination of strict and weighted queuing. Use the **no** form to restore the default weights.

#### SYNTAX

**queue weight** *weight0...weight7*

**no queue weight**

*weight0...weight7* - The ratio of weights for queues 0 - 7 determines the weights used by the WRR scheduler. (Range: 1-15)

#### DEFAULT SETTING

Weights 1, 2, 4, 6, 8, 10, 12, 14 are assigned to queues 0 - 7 respectively.

#### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

#### COMMAND USAGE

- This command shares bandwidth at the egress port by defining scheduling weights for Weighted Round-Robin, or the queuing mode that uses a combination of strict and weighted queuing (page 929).
- Bandwidth is allocated to each queue by calculating a precise number of bytes per second that will be serviced on each round.

#### EXAMPLE

The following example shows how to assign round-robin weights of 1 - 8 to the CoS priority queues 0 - 7.

```
Console(config)#interface ge1/1
Console(config-if)#queue weight 1 2 3 4 5 6 7 8
Console(config-if)#
```

#### RELATED COMMANDS

queue mode (929)
show queue weight (933)

### 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 then default switchport priority.

- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.

- The switch provides eight priority queues for each port. It can be configured to use strict priority queuing, Weighted Round Robin (WRR), or a combination of strict and weighted queuing using the queue mode command. Inbound frames that do not have VLAN tags are tagged with the input port's default ingress user priority, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in queue 2 of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

#### EXAMPLE

The following example shows how to set a default priority on port 3 to 5:

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport priority default 5
Console(config-if)#
```

#### RELATED COMMANDS

show interfaces switchport (817)

## show queue cos-map

This command shows the class of service priority map.

**SYNTAX**

**show queue cos-map** [*interface*]

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

**DEFAULT SETTING**

None

**COMMAND MODE**

Privileged Exec

**EXAMPLE**

```
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
 CoS Value:      0 1 2 3 4 5 6 7
 Priority Queue: 2 0 1 3 4 5 6 7
Console#
```

## show queue mode

This command shows the current queue mode.

**SYNTAX**

**show queue mode** *interface*

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

**COMMAND MODE**

Privileged Exec

**EXAMPLE**

```
Console#show queue mode ethernet 1/1
Unit   Port   queue mode
----   ----   ---------------
  1      1   Weighted Round Robin
Console#
```

**show queue weight** This command displays the weights used for the weighted queues.

### SYNTAX

**show queue mode** *interface*

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show queue weight ethernet 1/1
Information of Eth 1/1
 Queue ID  Weight
 --------  ------
       0      1
       1      2
       2      4
       3      6
       4      8
       5     10
       6     12
       7     14
Console#
```

## PRIORITY COMMANDS (LAYER 3 AND 4)

This section describes commands used to configure Layer 3 and 4 traffic priority mapping on the switch.

**Table 4: Priority Commands (Layer 3 and 4)**

| Command | Function | Mode |
|---|---|---|
| map ip dscp | Enables IP DSCP class of service mapping | GC |
| map ip port | Enables TCP/UDP class of service mapping | GC |
| map ip precedence | Enables IP precedence class of service mapping | GC |
| map ip dscp | Maps IP DSCP value to a class of service | IC |
| map ip port | Maps TCP/UDP socket to a class of service | IC |
| map ip precedence | Maps IP precedence value to a class of service | IC |
| show map ip dscp | Shows the IP DSCP map | PE |
| show map ip port | Shows the IP port map | PE |
| show map ip precedence | Shows the IP precedence map | PE |

## map ip dscp (Global Configuration)

This command enables IP DSCP mapping (i.e., Differentiated Services Code Point mapping). Use the **no** form to disable IP DSCP mapping.

#### SYNTAX

[**no**] **map ip dscp**

#### DEFAULT SETTING

Disabled

#### COMMAND MODE

Global Configuration

#### COMMAND USAGE

- The precedence for priority mapping is IP 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 DSCP mapping globally:

```
Console(config)#map ip dscp
Console(config)#
```

## 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 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)#
```

## map ip dscp (Interface Configuration)

This command sets IP DSCP priority (i.e., Differentiated Services Code Point priority). Use the **no** form to restore the default table.

### SYNTAX

**map ip dscp** *dscp-value* **cos** *cos-value*

**no map ip dscp**

*dscp-value* - 8-bit DSCP value. (Range: 0-63)

*cos-value* - Class-of-Service value (Range: 0-7)

### DEFAULT SETTING

The DSCP default values are defined in the following table. Note that all the DSCP values that are not specified are mapped to CoS value 0.

**Table 5: Mapping IP DSCP to CoS Values**

| IP DSCP Value | CoS Value |
|---|---|
| 0 | 0 |
| 8 | 1 |
| 10, 12, 14, 16 | 2 |
| 18, 20, 22, 24 | 3 |

**Table 5: Mapping IP DSCP to CoS Values**

| IP DSCP Value | CoS Value |
|---|---|
| 26, 28, 30, 32, 34, 36 | 4 |
| 38, 40, 42 | 5 |
| 48 | 6 |
| 46, 56 | 7 |

### COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE
- The precedence for priority mapping is IP 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 eight hardware priority queues.
- This command sets the IP DSCP priority for all interfaces.

### EXAMPLE
The following example shows how to map IP DSCP value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#
```

## map ip port (Interface Configuration)

This command sets 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: 0-65535)

*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.

- Up to 8 entries can be specified for IP Port priority mapping.
- 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 (Interface Configuration)

This command sets IP precedence priority (i.e., IP Type of Service priority). Use the **no** form to restore the default table.

#### SYNTAX

**map ip precedence** *ip-precedence-value* **cos** *cos-value*

**no map ip precedence**

*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.

**Table 6: Mapping IP Precedence to CoS Values**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **IP Precedence Value** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| **CoS Value** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

#### 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.
- 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.

#### EXAMPLE

The following example shows how to map IP precedence value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip precedence 1 cos 0
Console(config-if)#
```

## show map ip dscp

This command shows the IP DSCP priority map.

### SYNTAX

**show map ip dscp** [*interface*]

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

### 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#
```

## show map ip port

This command shows the IP port priority map.

### SYNTAX

**show map ip port** [*interface*]

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

### COMMAND MODE

Privileged Exec

### EXAMPLE

The following shows that HTTP traffic has been mapped to CoS value 0:

```
Console#show map ip port
TCP port mapping status: disabled

 Port      IP Port  CoS
 --------- -------- ---
  Eth 1/ 5       80   0
Console#
```

## show map ip precedence

This command shows the IP precedence priority map.

### SYNTAX

**show map ip precedence** [*interface*]

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

### 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#
```

# 41 QUALITY OF SERVICE COMMANDS

The commands described in this section are used to configure Differentiated Services (DiffServ) classification criteria and service policies. You can classify traffic based on access lists, IP Precedence or DSCP values, or VLANs. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet.

**Table 1: Quality of Service Commands**

| Command | Function | Mode |
|---|---|---|
| class-map | Creates a class map for a type of traffic | GC |
| description | Specifies the description of a class map | CM |
| match | Defines the criteria used to classify traffic | CM |
| rename | Redefines the name of a class map | CM |
| policy-map | Creates a policy map for multiple interfaces | GC |
| description | Specifies the description of a policy map | PM |
| class | Defines a traffic classification for the policy to act on | PM |
| rename | Redefines the name of a policy map | PM |
| police flow | Defines an enforcer for classified traffic based on a metered flow rate | PM-C |
| police srtcm-color | Defines an enforcer for classified traffic based on a single rate three color meter | PM-C |
| police trtcm-color | Defines an enforcer for classified traffic based on a two rate three color meter | PM-C |
| set | Classifies IP traffic by setting a CoS, DSCP, or IP-precedence value in a packet | PM-C |
| service-policy | Applies a policy map defined by the policy-map command to the input of a particular interface | IC |
| show class-map | Displays the QoS class maps which define matching criteria used for classifying traffic | PE |
| show policy-map | Displays the QoS policy maps which define classification criteria for incoming traffic, and may include policers for bandwidth limitations | PE |
| show policy-map interface | Displays the configuration of all classes configured for all service policies on the specified interface | PE |

To create a service policy for a specific category of ingress traffic, follow these steps:

1. Use the class-map command to designate a class name for a specific category of traffic, and enter the Class Map configuration mode.

2. Use the match command to select a specific type of traffic based on an access list, a DSCP or IP Precedence value, or a VLAN.

3. Use the policy-map command to designate a policy name for a specific manner in which ingress traffic will be handled, and enter the Policy Map configuration mode.

4. Use the class command to identify the class map, and enter Policy Map Class configuration mode. A policy map can contain up to 16 class maps.

5. Use the set command to modify theCoS value in the VLAN tag or the priority bits in the IP header for the matching traffic class, and use one of the **police** commands to monitor parameters such as the average flow and burst rate, and drop any traffic that exceeds the specified rate, or just reduce the DSCP service level for traffic exceeding the specified rate.

6. Use the service-policy command to assign a policy map to a specific interface.

**NOTE:** Create a Class Map before creating a Policy Map.

## class-map

This command creates a class map used for matching packets to the specified class, and enters Class Map configuration mode. Use the **no** form to delete a class map.

### SYNTAX

[**no**] **class-map** *class-map-name* [**match-any**]

*class-map-name* - Name of the class map. (Range: 1-16 characters)

**match-any** - Match any condition within a class map.

### DEFAULT SETTING

None

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- First enter this command to designate a class map and enter the Class Map configuration mode. Then use match commands to specify the criteria for ingress traffic that will be classified under this class map.

- One or more class maps can be assigned to a policy map.The policy map is then bound by a service policy to an interface. A service policy defines packet classification, service tagging, and bandwidth policing. Once a policy map has been bound to an interface, no additional class maps may be added to the policy map, nor any changes made to the assigned class maps with the match or set commands.

### EXAMPLE

This example creates a class map call “rd-class,” and sets it to match packets marked for DSCP service value 3:

```
Console(config)#class-map rd-class match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```

**RELATED COMMANDS**
show class-map

## description

This command specifies the description of a class map or policy map.

**SYNTAX**

**description** *string*

*string* - Description of the class map or policy map.
(Range: 1-64 characters)

**COMMAND MODE**
Class Map Configuration
Policy Map Configuration

**EXAMPLE**

```
Console(config)#class-map rd-class#1
Console(config-cmap)#description matches packets marked for DSCP service value 3
Console(config-cmap)#
```

## match

This command defines the criteria used to classify traffic. Use the **no** form to delete the matching criteria.

**SYNTAX**

[**no**] **match** {**access-list** *acl-name* | **ip dscp** *dscp* |
**ip precedence** *ip-precedence* | **ipv6 dscp** *dscp* | **vlan** *vlan*}

*acl-name* - Name of the access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs. (Range: 1-16 characters)

*dscp* - A Differentiated Service Code Point value. (Range: 0-63)

*ip-precedence* - An IP Precedence value. (Range: 0-7)

*vlan* - A VLAN. (Range:1-4093)

**DEFAULT SETTING**
None

**COMMAND MODE**
Class Map Configuration

### COMMAND USAGE

- First enter the class-map command to designate a class map and enter the Class Map configuration mode. Then use **match** commands to specify the fields within ingress packets that must match to qualify for this class map.
- If an ingress packet matches an ACL specified by this command, any deny rules included in the ACL will be ignored.
- If match criteria includes an IP ACL or IP priority rule, then a VLAN rule cannot be included in the same class map.
- If match criteria includes a MAC ACL or VLAN rule, then neither an IP ACL nor IP priority rule can be included in the same class map.
- Up to 16 match entries can be included in a class map.

### EXAMPLE

This example creates a class map called “rd-class#1,” and sets it to match packets marked for DSCP service value 3.

```
Console(config)#class-map rd-class#1 match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```

This example creates a class map call “rd-class#2,” and sets it to match packets marked for IP Precedence service value 5.

```
Console(config)#class-map rd-class#2 match-any
Console(config-cmap)#match ip precedence 5
Console(config-cmap)#
```

This example creates a class map call “rd-class#3,” and sets it to match packets marked for VLAN 1.

```
Console(config)#class-map rd-class#3 match-any
Console(config-cmap)#match vlan 1
Console(config-cmap)#
```

## rename

This command redefines the name of a class map or policy map.

### SYNTAX

**rename** *map-name*

*map-name* - Name of the class map or policy map. (Range: 1-16 characters)

#### COMMAND MODE
Class Map Configuration
Policy Map Configuration

#### EXAMPLE

```
Console(config)#class-map rd-class#1
Console(config-cmap)#rename rd-class#9
Console(config-cmap)#
```

### policy-map

This command creates a policy map that can be attached to multiple interfaces, and enters Policy Map configuration mode. Use the **no** form to delete a policy map.

#### SYNTAX

[**no**] **policy-map** *policy-map-name*

*policy-map-name* - Name of the policy map. (Range: 1-16 characters)

#### DEFAULT SETTING
None

#### COMMAND MODE
Global Configuration

#### COMMAND USAGE

- Use the **policy-map** command to specify the name of the policy map, and then use the class command to configure policies for traffic that matches the criteria defined in a class map.
- A policy map can contain multiple class statements that can be applied to the same interface with the service-policy command.
- Create a Class Map before assigning it to a Policy Map.

#### EXAMPLE
This example creates a policy called “rd-policy,” uses the class command to specify the previously defined “rd-class,” uses the **set** command to classify the service that incoming packets will receive, and then uses the police-flow command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police flow 10000 4000 conform-action transmit violate-action drop
Console(config-pmap-c)#
```

## class

This command defines a traffic classification upon which a policy can act, and enters Policy Map Class configuration mode. Use the **no** form to delete a class map.

### SYNTAX

[**no**] **class** *class-map-name*

*class-map-name* - Name of the class map. (Range: 1-16 characters)

### DEFAULT SETTING

None

### COMMAND MODE

Policy Map Configuration

### COMMAND USAGE

- Use the policy-map command to specify a policy map and enter Policy Map configuration mode. Then use the **class** command to enter Policy Map Class configuration mode. And finally, use the **set** command and one of the **police** commands to specify the match criteria, where the:
  - set command modifies the CoS value in the VLAN tag or the priority bits in the IP header for matching packets.
  - **police** commands define parameters such as the maximum throughput, burst rate, and response to non-conforming traffic.
- Up to 16 classes can be included in a policy map.

### EXAMPLE

This example creates a policy called “rd-policy,” uses the **class** command to specify the previously defined “rd-class,” uses the set command to classify the service that incoming packets will receive, and then uses the police flow command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4,000 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police flow 10000 4000 conform-action transmit violate-action drop
Console(config-pmap-c)#
```

## police flow

This command defines an enforcer for classified traffic based on the metered flow rate. Use the no form to remove a policer.

### SYNTAX

[**no**] **police flow** *committed-rate committed-burst*
**violate-action** {**drop**| *new-dscp*}

*committed-rate* - Committed information rate (CIR) in kilobits per second. (Range: 64-1000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

*committed-burst* - Committed burst size (BC) in bytes.
(Range: 4000-16000000 at a granularity of 4k bytes)

**violate-action** - Action to take when packet exceeds the CIR and BC. (There are not enough tokens to service the packet, the packet is set red).

**transmit** - Transmits without taking any action.

**drop** - Drops packet as required by violate-action.

*new-dscp* - Differentiated Service Code Point (DSCP) value. (Range: 0-63)

### DEFAULT SETTING

None

### COMMAND MODE

Policy Map Class Configuration

### COMMAND USAGE

- You can configure up to 16 policers (i.e., class maps) for ingress ports.

- The *committed-rate* cannot exceed the configured interface speed, and the *committed-burst* cannot exceed 16 Mbytes.

- Policing is based on a token bucket, where bucket depth (i.e., the maximum burst before the bucket overflows) is by specified the *committed-burst* field, and the average rate tokens are added to the bucket is by specified by the *committed-rate* option. Note that the token bucket functions similar to that described in RFC 2697 and RFC 2698.

- The behavior of the meter is specified in terms of one token bucket (C), the rate at which the tokens are incremented (CIR – Committed Information Rate), and the maximum size of the token bucket (BC – Committed Burst Size).

  The token bucket C is initially full, that is, the token count Tc(0) = BC. Thereafter, the token count Tc is updated CIR times per second as follows:

  - If Tc is less than BC, Tc is incremented by one, else
  - Tc is not incremented.

  When a packet of size B bytes arrives at time t, the following happens:

  - If Tc(t)-B ≥ 0, the packet is green and Tc is decremented by B down to the minimum value of 0, else
  - else the packet is red and Tc is not decremented.

### EXAMPLE

This example creates a policy called "rd-policy," uses the class command to specify the previously defined "rd-class," uses the set command to classify the service that incoming packets will receive, and then uses the **police flow** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police flow 100000 4000 violate-action drop
Console(config-pmap-c)#
```

## police srtcm-color

This command defines an enforcer for classified traffic based on a single rate three color meter (srTCM). Use the **no** form to remove a policer.

### SYNTAX

[**no**] **police** {**srtcm-color-blind** | **srtcm-color-aware**}
*committed-rate committed-burst excess-burst*
**exceed-action** {**drop** | *new-dscp*}
**violate action** {**drop** | *new-dscp*}

**srtcm-color-blind** - Single rate three color meter in color-blind mode.

**srtcm-color-aware** - Single rate three color meter in color-aware mode.

*committed-rate* - Committed information rate (CIR) in kilobits per second. (Range: 64-1000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

*committed-burst* - Committed burst size (BC) in bytes. (Range: 4000-16000000 at a granularity of 4k bytes)

*excess-burst* - Excess burst size (BE) in bytes. (Range: 4000-1600000 at a granularity of 4k bytes)

**exceed-action** - Action to take when rate exceeds the CIR and BC but is within the BE. (There are enough tokens in bucket BE to service the packet, the packet is set yellow.)

**violate-action** - Action to take when rate exceeds the BE. (There are not enough tokens in bucket BE to service the packet, the packet is set red.)

**transmit** - Transmits without taking any action.

**drop** - Drops packet as required by exceed-action or violate-action.

*new-dscp* - Differentiated Service Code Point (DSCP) value. (Range: 0-63)

### DEFAULT SETTING

None

### COMMAND MODE

Policy Map Class Configuration

**COMMAND USAGE**

- You can configure up to 16 policers (i.e., class maps) for ingress ports.

- The *committed-rate* cannot exceed the configured interface speed, and the *committed-burst* and *excess-burst* cannot exceed 16 Mbytes.

- The srTCM as defined in RFC 2697 meters a traffic stream and processes its packets according to three traffic parameters – Committed Information Rate (CIR), Committed Burst Size (BC), and Excess Burst Size (BE).

- The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. A packet is marked green if it doesn't exceed the CIR and BC, yellow if it does exceed the CIR and BC, but not the BE, and red otherwise.

- The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The marker (re)colors an IP packet according to the results of the meter. The color is coded in the DS field [RFC 2474] of the packet.

- The behavior of the meter is specified in terms of its mode and two token buckets, C and E, which both share the common rate CIR. The maximum size of the token bucket C is BC and the maximum size of the token bucket E is BE.

  The token buckets C and E are initially full, that is, the token count Tc(0) = BC and the token count Te(0) = BE. Thereafter, the token counts Tc and Te are updated CIR times per second as follows:

  - If Tc is less than BC, Tc is incremented by one, else
  - if Te is less then BE, Te is incremented by one, else
  - neither Tc nor Te is incremented.

  When a packet of size B bytes arrives at time t, the following happens if srTCM is configured to operate in color-blind mode:

  - If $Tc(t)-B \geq 0$, the packet is green and Tc is decremented by B down to the minimum value of 0, else
  - if $Te(t)-B \geq 0$, the packets is yellow and Te is decremented by B down to the minimum value of 0,
  - else the packet is red and neither Tc nor Te is decremented.

  When a packet of size B bytes arrives at time t, the following happens if srTCM is configured to operate in color-aware mode:

  - If the packet has been precolored as green and $Tc(t)-B \geq 0$, the packet is green and Tc is decremented by B down to the minimum value of 0, else
  - If the packet has been precolored as yellow or green and if
  - $Te(t)-B \geq 0$, the packets is yellow and Te is decremented by B down to the minimum value of 0, else the packet is red and neither Tc nor Te is decremented.

  The metering policy guarantees a deterministic behavior where the volume of green packets is never smaller than what has been determined by the CIR and

BC, that is, tokens of a given color are always spent on packets of that color. Refer to RFC 2697 for more information on other aspects of srTCM.

### EXAMPLE

This example creates a policy called "rd-policy," uses the class command to specify the previously defined "rd-class," uses the set command to classify the service that incoming packets will receive, and then uses the **police srtcm-color-blind** command to limit the average bandwidth to 100,000 Kbps, the committed burst rate to 4000 bytes, the excess burst rate to 6000 bytes, to remark any packets exceeding the committed burst size, and to drop any packets exceeding the excess burst size.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police srtcm-color-blind 100000 4000 6000 exceed-action 0 violate-action drop
Console(config-pmap-c)#
```

## police trtcm-color

This command defines an enforcer for classified traffic based on a two rate three color meter (trTCM). Use the **no** form to remove a policer.

### SYNTAX

[**no**] **police** {**trtcm-color-blind** | **trtcm-color-aware**}
*committed-rate committed-burst peak-rate peak-burst*
**exceed-action** {**drop** | *new-dscp*}
**violate action** {**drop** | *new-dscp*}

**trtcm-color-blind** - Two rate three color meter in color-blind mode.

**trtcm-color-aware**- Two rate three color meter in color-aware mode.

*committed-rate* - Committed information rate (CIR) in kilobits per second. (Range: 64-1000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

*committed-burst*- Committed burst size (BC) in bytes. (Range: 4000-16000000 at a granularity of 4k bytes)

*peak-rate* - Peak information rate(PIR) in kilobits per second. (Range: 64-1000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

*peak-burst* - Burst size (BP) in bytes. (Range: 4000-16000000 at a granularity of 4k bytes)

**exceed-action** - Action to take when rate exceeds the CIR but is within the PIR. (Packet size exceeds BC but there are enough tokens in bucket BP to service the packet, the packet is set yellow.)

**violate-action** - Action to take when rate exceeds the PIR. (There are not enough tokens in bucket BP to service the packet, the packet is set red.)

**transmit** - Transmits without taking any action.

**drop** - Drops packet as required by exceed-action or violate-action.

*new-dscp* - Differentiated Service Code Point (DSCP) value. (Range: 0-63)

### DEFAULT SETTING
None

### COMMAND MODE
Policy Map Class Configuration

### COMMAND USAGE
- You can configure up to 16 policers (i.e., class maps) for ingress ports.
- The *committed-rate* and *peak-rate* cannot exceed the configured interface speed, and the *committed-burst* and *peak-burst* cannot exceed 16 Mbytes.
- The trTCM as defined in RFC 2698 meters a traffic stream and processes its packets based on two rates – Committed Information Rate (CIR) and Peak Information Rate (PIR), and their associated burst sizes - Committed Burst Size (BC) and Peak Burst Size (BP).
- The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. A packet is marked red if it exceeds the PIR. Otherwise it is marked either yellow or green depending on whether it exceeds or doesn't exceed the CIR.

  The trTCM is useful for ingress policing of a service, where a peak rate needs to be enforced separately from a committed rate.
- The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The marker (re)colors an IP packet according to the results of the meter. The color is coded in the DS field [RFC 2474] of the packet.
- The behavior of the meter is specified in terms of its mode and two token buckets, P and C, which are based on the rates PIR and CIR, respectively. The maximum size of the token bucket P is BP and the maximum size of the token bucket C is BC.
- The token buckets P and C are initially (at time 0) full, that is, the token count Tp(0) = BP and the token count Tc(0) = BC. Thereafter, the token count Tp is incremented by one PIR times per second up to BP and the token count Tc is incremented by one CIR times per second up to BC.

  When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in color-blind mode:

  - If Tp(t)-B < 0, the packet is red, else
  - if Tc(t)-B < 0, the packet is yellow and Tp is decremented by B, else
  - the packet is green and both Tp and Tc are decremented by B.

  When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in color-aware mode:

  - If the packet has been precolored as red or if Tp(t)-B < 0, the packet is red, else

- if the packet has been precolored as yellow or if Tc(t)-B < 0, the packet is yellow and Tp is decremented by B, else
- the packet is green and both Tp and Tc are decremented by B.

- The trTCM can be used to mark a IP packet stream in a service, where different, decreasing levels of assurances (either absolute or relative) are given to packets which are green, yellow, or red. Refer to RFC 2698 for more information on other aspects of trTCM.

#### EXAMPLE

This example creates a policy called “rd-policy,” uses the class command to specify the previously defined “rd-class,” uses the set command to classify the service that incoming packets will receive, and then uses the **police trtcm-color-blind** command to limit the average bandwidth to 100,000 Kbps, the committed burst rate to 4000 bytes, the peak information rate to 1,000,000 kbps, the peak burst size to 6000, to remark any packets exceeding the committed burst size, and to drop any packets exceeding the peak information rate.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police trtcm-color-blind 100000 4000 100000 6000 exceed-action 0 violate-
   action drop
Console(config-pmap-c)#
```

### set

This command modifies the CoS, DSCP or IP Precedence value in a matching packet (as specified by the match command). Use the **no** form to remove this traffic classification.

#### SYNTAX

[**no**] **set** {**cos** *new-cos* | **ip dscp** *new-dscp* | **ip precedence** *new-ip-precedence*}

*new-cos* - New Class of Service (CoS) value. (Range: 0-7)

*new-dscp* - New Differentiated Service Code Point (DSCP) value. (Range: 0-63)

*new-ip-precedence* - New IP Precedence value. (Range: 0-7)

#### DEFAULT SETTING

None

#### COMMAND MODE

Policy Map Class Configuration

#### COMMAND USAGE

- The **set cos** command is used to set the CoS value in the VLAN tag for matching packets.

- The **set ip dscp** and **set ip precedence** commands are used to set these priority values in the packet’s ToS field for matching packets.

- Each of these commands function at the same level of priority. Therefore setting any one of these commands will overwrite the action configured by the last **set** command.

### EXAMPLE

This example creates a policy called “rd-policy,” uses the class command to specify the previously defined “rd-class,” uses the **set cos** command to classify the service that incoming packets will receive, and then uses the police flow command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set cos 3
Console(config-pmap-c)#police flow 10000 4000 conform-action transmit violate-action drop
Console(config-pmap-c)#
```

## service-policy

This command applies a policy map defined by the **policy-map** command to the ingress side of a particular interface. Use the **no** form to remove this mapping.

### SYNTAX

[**no**] **service-policy input** *policy-map-name*

**input** - Apply to the input traffic.

*policy-map-name* - Name of the policy map for this interface. (Range: 1-32 characters)

### DEFAULT SETTING

No policy map is attached to an interface.

### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE

- Only one policy map can be assigned to an interface.
- First define a class map, then define a policy map, and finally use the **service-policy** command to bind the policy map to the required interface.
- The switch does not allow a policy map to be bound to an interface for egress traffic.

### EXAMPLE

This example applies a service policy to an ingress interface.

```
Console(config)#interface ethernet 1/1
Console(config-if)#service-policy input rd-policy
Console(config-if)#
```

## show class-map

This command displays the QoS class maps which define matching criteria used for classifying traffic.

### SYNTAX

**show class-map** [*class-map-name*]

*class-map-name* - Name of the class map. (Range: 1-32 characters)

### DEFAULT SETTING

Displays all class maps.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show class-map
Class Map match-any rd-class#1
Description:
 Match ip dscp 10
 Match access-list rd-access
 Match ip dscp 0

Class Map match-any rd-class#2
 Match ip precedence 5

Class Map match-any rd-class#3
 Match vlan 1

Console#
```

## show policy-map

This command displays the QoS policy maps which define classification criteria for incoming traffic, and may include policers for bandwidth limitations.

### SYNTAX

**show policy-map** [*policy-map-name* [**class** *class-map-name*]]

*policy-map-name* - Name of the policy map.
(Range: 1-16 characters)

*class-map-name* - Name of the class map. (Range: 1-16 characters)

### DEFAULT SETTING

Displays all policy maps and all classes.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show policy-map
Policy Map rd-policy
Description:
 class rd-class
```

```
 set cos 3
Console#show policy-map rd-policy class rd-class
Policy Map rd-policy
 class rd-class
 set cos 3
Console#
```

## show policy-map interface

This command displays the service policy assigned to the specified interface.

### SYNTAX

**show policy-map interface** *interface* **input**

*interface*

*unit/port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show policy-map interface 1/5 input
Service-policy rd-policy
Console#
```

# 42 MULTICAST FILTERING COMMANDS

This switch uses IGMP (Internet Group Management Protocol) to check 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.

Note that IGMP query can be enabled globally at Layer 2, or enabled for specific VLAN interfaces at Layer 3. (Layer 2 query is disabled if Layer 3 query is enabled.)

**Table 1: Multicast Filtering Commands**

| Command Group | Function |
|---|---|
| IGMP Snooping | Configures multicast groups via IGMP snooping or static assignment, sets the IGMP version, enables proxy reporting, displays current snooping settings, and displays the multicast service and group members |
| Static Multicast Routing | Configures static multicast router ports which forward all inbound multicast traffic to the attached VLANs |
| IGMP Filtering and Throttling | Configures IGMP filtering and throttling |
| Multicast VLAN Registration | Configures a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, preserving security and data isolation for normal traffic |
| IGMP (Layer 3) | Configures the IGMP protocol used with multicast routing in IPv4 networks |
| IGMP Proxy Routing | Collects and sends multicast group membership information onto the upstream interface based on IGMP messages monitored on downstream interfaces, and forwards multicast traffic based on that information |
| MLD (Layer 3) | Configures the MLD protocol used with multicast routing in IPv6 networks |
| MLD Proxy Routing | Collects and sends multicast group membership information onto the upstream interface based on MLD messages monitored on downstream interfaces, and forwards multicast traffic based on that information |

## IGMP SNOOPING

This section describes commands used to configure IGMP snooping on the switch.

**Table 2: IGMP Snooping Commands**

| Command | Function | Mode |
|---|---|---|
| ip igmp snooping | Enables IGMP snooping | GC |
| ip igmp snooping proxy-reporting | Enables IGMP Snooping with Proxy Reporting | GC |
| ip igmp snooping querier | Allows this device to act as the querier for IGMP snooping | GC |
| ip igmp snooping router-alert-option-check | Discards any IGMPv2/v3 packets that do not include the Router Alert option | GC |

**Table 2: IGMP Snooping Commands (Continued)**

| Command | Function | Mode |
|---|---|---|
| ip igmp snooping router-port-expire-time | Configures the querier timeout | GC |
| ip igmp snooping tcn-flood | Floods multicast traffic when a Spanning Tree topology change occurs | GC |
| ip igmp snooping tcn-query-solicit | Sends an IGMP Query Solicitation when a Spanning Tree topology change occurs | GC |
| ip igmp snooping unregistered-data-flood | Floods unregistered multicast traffic into the attached VLAN | GC |
| ip igmp snooping unsolicited-report-interval | Specifies how often the upstream interface should transmit unsolicited IGMP reports (when report suppression/proxy reporting is enabled) | GC |
| ip igmp snooping version | Configures the IGMP version for snooping | GC |
| ip igmp snooping version-exclusive | Discards received IGMP messages which use a version different to that currently configured | GC |
| ip igmp snooping vlan general-query-suppression | Suppresses general queries except for ports attached to downstream multicast hosts | GC |
| ip igmp snooping vlan immediate-leave | Immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate-leave is enabled for the parent VLAN | GC |
| ip igmp snooping vlan last-memb-query-count | Configures the number of IGMP proxy query messages that are sent out before the system assumes there are no local members | GC |
| ip igmp snooping vlan last-memb-query-intvl | Configures the last-member-query interval | GC |
| ip igmp snooping vlan mrd | Sends multicast router solicitation messages | GC |
| ip igmp snooping vlan proxy-address | Configures a static address for proxy IGMP query and reporting | GC |
| ip igmp snooping vlan proxy-reporting | Enables IGMP Snooping with Proxy Reporting | GC |
| ip igmp snooping vlan query-interval | Configures the interval between sending IGMP proxy general queries | GC |
| ip igmp snooping vlan query-resp-intvl | Configures the maximum time the system waits for a response to proxy general queries | GC |
| ip igmp snooping vlan static | Adds an interface as a member of a multicast group | GC |
| ip igmp snooping vlan version | Configures the IGMP version for snooping | GC |
| ip igmp snooping vlan version-exclusive | Discards received IGMP messages which use a version different to that currently configured | GC |
| show ip igmp snooping | Shows the IGMP snooping, proxy, and query configuration | PE |
| show ip igmp snooping group | Shows known multicast group, source, and host port mapping | PE |
| show mac-address-table multicast | Shows known multicast addresses | PE |

## ip igmp snooping

This command enables IGMP snooping globally on the switch or on a selected VLAN interface. Use the **no** form to disable it.

#### SYNTAX

[**no**] **ip igmp snooping** [**vlan** *vlan-id*]

*vlan-id* - VLAN ID (Range: 1-4093)

#### DEFAULT SETTING

Enabled

#### COMMAND MODE

Global Configuration

#### COMMAND USAGE

- When IGMP snooping is enabled globally, the per VLAN interface settings for IGMP snooping take precedence.
- When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.

#### EXAMPLE

The following example enables IGMP snooping globally.

```
Console(config)#ip igmp snooping
Console(config)#
```

## ip igmp snooping proxy-reporting

This command enables IGMP Snooping with Proxy Reporting. Use the **no** form to restore the default setting.

#### SYNTAX

[**no**] **ip igmp snooping proxy-reporting**

**ip igmp snooping vlan** *vlan-id* **proxy-reporting** {**enable** | **disable**}
**no ip igmp snooping vlan** *vlan-id* **proxy-reporting**

*vlan-id* - VLAN ID (Range: 1-4093)

**enable** - Enable on the specified VLAN.

**disable** - Disable on the specified VLAN.

#### DEFAULT SETTING

Global: Enabled
VLAN: Based on global setting

#### COMMAND MODE

Global Configuration

#### COMMAND USAGE

- When proxy reporting is enabled with this command, the switch performs “IGMP Snooping with Proxy Reporting” (as defined in DSL Forum TR-101, April 2006), including report suppression, last leave, and query suppression. Report suppression intercepts, absorbs and summarizes IGMP reports coming from downstream hosts. Last leave sends out a proxy query when the last member leaves a multicast group, and query suppression means that neither specific queries nor general queries are forwarded from an upstream multicast router to hosts downstream from this device.

- If the IGMP proxy reporting is configured on a VLAN, this setting takes precedence over the global configuration.

#### EXAMPLE

```
Console(config)#ip igmp snooping proxy-reporting
Console(config)#
```

## ip igmp snooping querier

This command enables the switch as an IGMP querier. Use the **no** form to disable it.

#### SYNTAX

[**no**] **ip igmp snooping querier**

#### DEFAULT SETTING

Enabled

#### COMMAND MODE

Global Configuration

#### COMMAND USAGE

- IGMP snooping querier is not supported for IGMPv3 snooping (see ip igmp snooping version).
- 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)#
```

## ip igmp snooping router-alert-option-check

This command discards any IGMPv2/v3 packets that do not include the Router Alert option. Use the **no** form to ignore the Router Alert Option when receiving IGMP messages.

#### SYNTAX

[**no**] **ip igmp snooping router-alert-option-check**

#### DEFAULT SETTING

Disabled

#### COMMAND MODE
Global Configuration

#### COMMAND USAGE
As described in Section 9.1 of RFC 3376 for IGMP Version 3, the Router Alert Option can be used to protect against DOS attacks. One common method of attack is launched by an intruder who takes over the role of querier, and starts overloading multicast hosts by sending a large number of group-and-source-specific queries, each with a large source list and the Maximum Response Time set to a large value.

To protect against this kind of attack, (1) routers should not forward queries. This is easier to accomplish if the query carries the Router Alert option. (2) Also, when the switch is acting in the role of a multicast host (such as when using proxy routing), it should ignore version 2 or 3 queries that do not contain the Router Alert option.

#### EXAMPLE

```
Console(config)#ip igmp snooping router-alert-option-check
Console(config)#
```

### ip igmp snooping router-port-expire-time

This command configures the querier timeout. Use the **no** form to restore the default.

#### SYNTAX

**ip igmp snooping router-port-expire-time** *seconds*

**no ip igmp snooping router-port-expire-time**

*seconds* - The time the switch waits after the previous querier stops before it considers it to have expired. (Range: 1-65535; Recommended Range: 300-500)

#### DEFAULT SETTING
300 seconds

#### COMMAND MODE
Global Configuration

#### EXAMPLE
The following shows how to configure the timeout to 400 seconds:

```
Console(config)#ip igmp snooping router-port-expire-time 400
Console(config)#
```

### ip igmp snooping tcn-flood

This command enables flooding of multicast traffic if a spanning tree topology change notification (TCN) occurs. Use the **no** form to disable flooding.

#### SYNTAX

[**no**] **ip igmp snooping tcn-flood**

### DEFAULT SETTING
Disabled

### COMMAND MODE
Global Configuration

### COMMAND USAGE
- When a spanning tree topology change occurs, the multicast membership information learned by the switch may be out of date. For example, a host linked to one port before the topology change (TC) may be moved to another port after the change. To ensure that multicast data is delivered to all receivers, by default, a switch in a VLAN (with IGMP snooping enabled) that receives a Bridge Protocol Data Unit (BPDU) with the TC bit set (by the root bridge) will enter into “multicast flooding mode” for a period of time until the topology has stabilized and the new locations of all multicast receivers are learned.

- If a topology change notification (TCN) is received, and all the uplink ports are subsequently deleted, a timeout mechanism is used to delete all of the currently learned multicast channels.

- When a new uplink port starts up, the switch sends unsolicited reports for all current learned channels out through the new uplink port.

- By default, the switch immediately enters into “multicast flooding mode” when a spanning tree topology change occurs. In this mode, multicast traffic will be flooded to all VLAN ports. If many ports have subscribed to different multicast groups, flooding may cause excessive loading on the link between the switch and the end host. Flooding may be disabled to avoid this, causing multicast traffic to be delivered only to those ports on which multicast group members have been learned.

- When the spanning tree topology changes, the root bridge sends a proxy query to quickly re-learn the host membership/port relations for multicast channels. The root bridge also sends an unsolicited Multicast Router Discover (MRD) request to quickly locate the multicast routers in this VLAN.

  The proxy query and unsolicited MRD request are flooded to all VLAN ports except for the receiving port when the switch receives such packets.

### EXAMPLE
The following example enables TCN flooding.

```
Console(config)#ip igmp snooping tcn-flood
Console(config)#
```

## ip igmp snooping tcn-query-solicit

This command instructs the switch to send out an IGMP general query solicitation when a spanning tree topology change notification (TCN) occurs. Use the **no** form to disable this feature.

### SYNTAX

[**no**] **ip igmp snooping tcn-query-solicit**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- When the root bridge in a spanning tree receives a topology change notification for a VLAN where IGMP snooping is enabled, it issues a global IGMP leave message (query solicitation). When a switch receives this solicitation, it floods it to all ports in the VLAN where the spanning tree change occurred. When an upstream multicast router receives this solicitation, it will also immediately issues an IGMP general query.
- The **ip igmp snooping tcn query-solicit** command can be used to send a query solicitation whenever it notices a topology change, even if the switch is not the root bridge in the spanning tree.

### EXAMPLE

The following example instructs the switch to issue an IGMP general query whenever it receives a spanning tree topology change notification.

```
Console(config)#ip igmp snooping tcn query-solicit
Console(config)#
```

## ip igmp snooping unregistered-data-flood

This command floods unregistered multicast traffic into the attached VLAN. Use the **no** form to drop unregistered multicast traffic.

### SYNTAX

[**no**] **ip igmp snooping unregistered-data-flood**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Global Configuration

### COMMAND USAGE

Once the table used to store multicast entries for IGMP snooping and multicast routing is filled, no new entries are learned. If no router port is configured in the attached

VLAN, and unregistered-flooding is disabled, any subsequent multicast traffic not found in the table is dropped, otherwise it is flooded throughout the VLAN.

### EXAMPLE

```
Console(config)#ip igmp snooping unregistered-data-flood
Console(config)#
```

## ip igmp snooping unsolicited-report-interval

This command specifies how often the upstream interface should transmit unsolicited IGMP reports when report suppression/proxy reporting is enabled. Use the **no** form to restore the default value.

### SYNTAX

**ip igmp snooping unsolicited-report-interval** *seconds*

**no ip igmp snooping version-exclusive**

*seconds* - The interval at which to issue unsolicited reports. (Range: 1-65535 seconds)

### DEFAULT SETTING

400 seconds

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- When a new upstream interface (that is, uplink port) starts up, the switch sends unsolicited reports for all currently learned multicast channels out through the new upstream interface.
- This command only applies when proxy reporting is enabled (see page 959).

### EXAMPLE

```
Console(config)#ip igmp snooping unsolicited-report-interval 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** [**vlan** *vlan-id*] **version** {**1** | **2** | **3**}

**no ip igmp snooping version**

**vlan-id** - VLAN ID (Range: 1-4093)

**1** - IGMP Version 1

**2** - IGMP Version 2

**3** - IGMP Version 3

**DEFAULT SETTING**
Global: IGMP Version 2
VLAN: Not configured, based on global setting

**COMMAND MODE**
Global Configuration

**COMMAND USAGE**

- This command configures the IGMP report/query version used by IGMP snooping. Versions 1 - 3 are all supported, and versions 2 and 3 are backward compatible, so the switch can operate with other devices, regardless of the snooping version employed.

- If the IGMP snooping version is configured on a VLAN, this setting takes precedence over the global configuration.

**EXAMPLE**
The following configures the global setting for IGMP snooping to version 1.

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

## ip igmp snooping version-exclusive

This command discards any received IGMP messages (except for multicast protocol packets) which use a version different to that currently configured by the ip igmp snooping version command. Use the **no** form to disable this feature.

**SYNTAX**

**ip igmp snooping** [**vlan** *vlan-id*] **version-exclusive**

**no ip igmp snooping version-exclusive**

*vlan-id* - VLAN ID (Range: 1-4093)

**DEFAULT SETTING**
Global: Disabled
VLAN: Disabled

**COMMAND MODE**
Global Configuration

**COMMAND USAGE**

- If version exclusive is disabled on a VLAN, then this setting is based on the global setting. If it is enabled on a VLAN, then this setting takes precedence over the global setting.

- When this function is disabled, the currently selected version is backward compatible (see the ip igmp snooping version command.

### EXAMPLE

```
Console(config)#ip igmp snooping version-exclusive
Console(config)#
```

## ip igmp snooping vlan general-query-suppression

This command suppresses general queries except for ports attached to downstream multicast hosts. Use the **no** form to flood general queries to all ports except for the multicast router port.

### SYNTAX

[**no**] **ip igmp snooping vlan** *vlan-id* **general-query-suppression**

*vlan-id* - VLAN ID (Range: 1-4093)

### DEFAULT SETTING

Disabled

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- By default, general query messages are flooded to all ports, except for the multicast router through which they are received.
- If general query suppression is enabled, then these messages are forwarded only to downstream ports which have joined a multicast service.

### EXAMPLE

```
Console(config)#ip igmp snooping vlan 1 general-query-suppression
Console(config)#
```

## ip igmp snooping vlan immediate-leave

This command immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate-leave is enabled for the parent VLAN. Use the **no** form to restore the default.

### SYNTAX

[**no**] **ip igmp snooping vlan** *vlan-id* **immediate-leave**

*vlan-id* - VLAN ID (Range: 1-4093)

### DEFAULT SETTING

Disabled

### COMMAND MODE

Global Configuration

**COMMAND USAGE**

- If immediate-leave is *not* used, a multicast router (or querier) will send a group-specific query message when an IGMPv2/v3 group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the timeout period. (The timeout for this release is currently defined by ip igmp snooping vlan last-memb-query-intvl * ip igmp robustval.

- If immediate-leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one IGMP-enabled device, either a service host or a neighbor running IGMP snooping.

- This command is only effective if IGMP snooping is enabled, and IGMPv2 or IGMPv3 snooping is used.

**EXAMPLE**

The following shows how to enable immediate leave.

```
Console(config)#ip igmp snooping vlan 1 immediate-leave
Console(config)#
```

## ip igmp snooping vlan last-memb-query-count

This command configures the number of IGMP proxy group-specific or group-and-source-specific query messages that are sent out before the system assumes there are no more local members. Use the **no** form to restore the default.

**SYNTAX**

**ip igmp snooping vlan** *vlan-id* **last-memb-query-count** *count*

**no ip igmp snooping vlan** *vlan-id* **last-memb-query-count**

*vlan-id* - VLAN ID (Range: 1-4093)

*count* - The number of proxy group-specific or group-and-source-specific query messages to issue before assuming that there are no more group members. (Range: 1-255)

**DEFAULT SETTING**

2

**COMMAND MODE**

Global Configuration

**COMMAND USAGE**

This command will take effect only if IGMP snooping proxy reporting is enabled (page 959).

**EXAMPLE**

```
Console(config)#ip igmp snooping vlan 1 last-memb-query-count 7
Console(config)#
```

## ip igmp snooping vlan last-memb-query-intvl

This command configures the last-member-query interval. Use the **no** form to restore the default.

### SYNTAX

**ip igmp snooping vlan** *vlan-id* **last-memb-query-intvl** *interval*

**no ip igmp snooping vlan** *vlan-id* **last-memb-query-intvl**

*vlan-id* - VLAN ID (Range: 1-4093)

*interval* - The interval to wait for a response to a group-specific or group-and-source-specific query message. (Range: 1-31744 tenths of a second)

### DEFAULT SETTING

10 (1 second)

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- When a multicast host leaves a group, it sends an IGMP leave message. When the leave message is received by the switch, it checks to see if this host is the last to leave the group by sending out an IGMP group-specific or group-and-source-specific query message, and starts a timer. If no reports are received before the timer expires, the group record is deleted, and a report is sent to the upstream multicast router.
- A reduced value will result in reduced time to detect the loss of the last member of a group or source, but may generate more bursty traffic.
- This command will take effect only if IGMP snooping proxy reporting is enabled (page 959).

### EXAMPLE

```
Console(config)#ip igmp snooping vlan 1 last-memb-query-intvl 700
Console(config)#
```

## ip igmp snooping vlan mrd

This command enables sending of multicast router solicitation messages. Use the **no** form to disable these messages.

### SYNTAX

[**no**] **ip igmp snooping vlan** *vlan-id* **mrd**

*vlan-id* - VLAN ID (Range: 1-4093)

### DEFAULT SETTING

Enabled

### COMMAND MODE

Global Configuration

#### COMMAND USAGE

- Multicast Router Discovery (MRD) uses multicast router advertisement, multicast router solicitation, and multicast router termination messages to discover multicast routers. Devices send solicitation messages in order to solicit advertisement messages from multicast routers. These messages are used to discover multicast routers on a directly attached link. Solicitation messages are also sent whenever a multicast forwarding interface is initialized or re-initialized. Upon receiving a solicitation on an interface with IP multicast forwarding and MRD enabled, a router will respond with an advertisement.

- Advertisements are sent by routers to advertise that IP multicast forwarding is enabled. These messages are sent unsolicited periodically on all router interfaces on which multicast forwarding is enabled. They are sent upon the expiration of a periodic timer, as a part of a router's start up procedure, during the restart of a multicast forwarding interface, and on receipt of a solicitation message. When the multicast services provided to a VLAN is relatively stable, the use of solicitation messages is not required and may be disabled using the **no ip igmp snooping vlan mrd** command.

- This command may also be used to disable multicast router solicitation messages when the upstream router does not support MRD, to reduce the loading on a busy upstream router, or when IGMP snooping is disabled in a VLAN.

#### EXAMPLE

This example disables sending of multicast router solicitation messages on VLAN 1.

```
Console(config)#no ip igmp snooping vlan 1 mrd
Console(config)#
```

### ip igmp snooping vlan proxy-address

This command configures a static source address for locally generated query and report messages used by IGMP proxy reporting. Use the **no** form to restore the default source address.

#### SYNTAX

[**no**] **ip igmp snooping vlan** *vlan-id* **proxy-address** *source-address*

*vlan-id* - VLAN ID (Range: 1-4093)

*source-address* - The source address used for proxied IGMP query and report, and leave messages. (Any valid IP unicast address)

#### DEFAULT SETTING

0.0.0.0

#### COMMAND MODE

Global Configuration

#### COMMAND USAGE

IGMP Snooping uses a null IP address of 0.0.0.0 for the source of IGMP query messages which are proxied to downstream hosts to indicate that it is not the elected querier, but is only proxying these messages as defined in RFC 4541. The switch also uses a null address in IGMP reports sent to upstream ports.

Many hosts do not implement RFC 4541, and therefore do not understand query messages with the source address of 0.0.0.0. These hosts will therefore not reply to the queries, causing the multicast router to stop sending traffic to them.

To resolve this problem, the source address in proxied IGMP query and report messages can be replaced with any valid unicast address (other than the router's own address) using this command.

#### EXAMPLE

The following example sets the source address for proxied IGMP query messages to 10.0.1.8.

```
Console(config)#ip igmp snooping vlan 1 proxy-address 10.0.1.8
Console(config)#
```

### ip igmp snooping vlan query-interval

This command configures the interval between sending IGMP general queries. Use the **no** form to restore the default.

#### SYNTAX

**ip igmp snooping vlan** *vlan-id* **query-interval** *interval*

**no ip igmp snooping vlan** *vlan-id* **query-interval**

*vlan-id* - VLAN ID (Range: 1-4093)

*interval* - The interval between sending IGMP general queries. (Range: 10-31744 seconds)

#### DEFAULT SETTING

100 (10 seconds)

#### COMMAND MODE

Global Configuration

#### COMMAND USAGE

- An IGMP general query message is sent by the switch at the interval specified by this command. When this message is received by downstream hosts, all receivers build an IGMP report for the multicast groups they have joined.
- This command applies when the switch is serving as the querier (page 960), or as a proxy host when IGMP snooping proxy reporting is enabled (page 959).

#### EXAMPLE

```
Console(config)#ip igmp snooping vlan 1 query-interval 150
Console(config)#
```

## ip igmp snooping vlan query-resp-intvl

This command configures the maximum time the system waits for a response to general queries. Use the **no** form to restore the default.

### SYNTAX

**ip igmp snooping vlan** *vlan-id* **query-resp-intvl** *interval*

**no ip igmp snooping vlan** *vlan-id* **query-resp-intvl**

*vlan-id* - VLAN ID (Range: 1-4093)

*interval* - The maximum time the system waits for a response to general queries. (Range: 10-31744 tenths of a second)

### DEFAULT SETTING

100 (10 seconds)

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- This command applies when the switch is serving as the querier (page 960), or as a proxy host when IGMP snooping proxy reporting is enabled (page 959).

### EXAMPLE

```
Console(config)#ip igmp snooping vlan 1 query-resp-intvl 20
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: 1-4093)

*ip-address* - IP address for multicast group

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

### DEFAULT SETTING

None

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- Static multicast entries are never aged out.

- When a multicast entry is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

**EXAMPLE**
The following shows how to statically configure a multicast group on a port.

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet 1/5
Console(config)#
```

## show ip igmp snooping

This command shows the IGMP snooping, proxy, and query configuration settings.

**COMMAND MODE**
Privileged Exec

**COMMAND USAGE**
This command displays global and VLAN-specific IGMP configuration settings. See Configuring IGMP Snooping and Query Parameters for a description of the displayed items.

**EXAMPLE**
The following shows the current IGMP snooping configuration:

```
Console#show ip igmp snooping
 IGMP snooping                  : Enabled
 Router port expire time        : 300 s
 Router alert check             : Disabled
 Tcn flood                      : Disabled
 Tcn query solicit              : Disabled
 Unregistered data flood        : Disabled
 Unsolicited report interval    : 400 s
 Version exclusive              : Disabled
 Version                        : 2
 Proxy reporting                : Enabled
 Querier                        : Disabled

 Vlan 1:
 --------
 IGMP snooping                  : Enabled
 IGMP snooping running status   : Inactive
 Version                        : Using global version (2)
 Version exclusive              : Using global status (Disabled)
 Immediate leave                : Disabled
 Last member query interval     : 10 (1/10s)
 Last member query count        : 2
 General query suppression      : Disabled
 Query interval                 : 125
 Query response interval        : 100 (1/10s)
 Proxy query address            : 0.0.0.0
 Proxy reporting                : Using global status (Disabled)
 Multicast Router Discovery     : Enabled
.
.
.
```

## show ip igmp snooping group

This command shows known multicast group, source, and host port mappings for the specified VLAN interface, or for all interfaces if none is specified.

### SYNTAX

**show ip igmp snooping group** [**vlan** *vlan-id* [**user** | **igmp-snp**]] [**user** | **igmpsnp**]

*vlan-id* - VLAN ID (1-4093)

**user** - Display only the user-configured multicast entries.

**igmpsnp** - 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 ip igmp snooping group vlan 1
VLAN     Group            Source           Port List
-------- ---------------- ---------------- ---------------------------------
       1 239.255.255.250  *                Eth1/ 1(D) Eth1/13(D)
       1 224.1.1.12       *                Eth 1/23(D)
Console#
```

## show mac-address-table multicast

This command shows known multicast addresses.

### SYNTAX

**show mac-address-table multicast** [**vlan** *vlan-id* [**user** | **igmp-snp**]] [**user** | **igmp-snooping**]

*vlan-id* - VLAN ID (1 to 4093)

**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
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1      224.1.2.3      Eth1/11    IGMP
Console#
```

## STATIC MULTICAST ROUTING

This section describes commands used to configure static multicast routing on the switch.

**Table 3: Static Multicast Interface Commands**

| Command | Function | Mode |
|---|---|---|
| ip igmp snooping vlan mrouter | Adds a multicast router port | GC |
| show ip igmp snooping mrouter | Shows multicast router ports | PE |

### ip igmp snooping vlan mrouter

This command statically configures a (Layer 2) multicast router port on the specified VLAN. Use the **no** form to remove the configuration.

### SYNTAX

[**no**] **ip igmp snooping vlan** *vlan-id* **mrouter** *interface*

*vlan-id* - VLAN ID (Range: 1-4093)

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

### DEFAULT SETTING

No static multicast router ports are configured.

### COMMAND MODE

Global Configuration

### COMMAND USAGE

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router or switch connected over the network to an interface (port or trunk) on this switch, that interface can be manually configured to join all the current multicast groups.

#### EXAMPLE

The following shows how to configure port 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: 1-4093)

#### DEFAULT SETTING

Displays multicast router ports for all configured VLANs.

#### COMMAND MODE

Privileged Exec

#### COMMAND USAGE

Multicast router port types displayed include Static or Dynamic.

#### EXAMPLE

The following shows the ports in VLAN 1 which are attached to multicast routers.

```
Console#show ip igmp snooping mrouter vlan 1
 VLAN M'cast Router Port Type
 ---- ------------------ -------
    1         Eth 1/11  Static
    2         Eth 1/12  Dynamic
Console#
```

## IGMP FILTERING AND THROTTLING

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The IGMP filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and IGMP throttling limits the number of simultaneous multicast groups a port can join.

**Table 4: IGMP Filtering and Throttling Commands**

| Command | Function | Mode |
|---|---|---|
| ip igmp filter | Enables IGMP filtering and throttling on the switch | GC |
| ip igmp profile | Sets a profile number and enters IGMP filter profile configuration mode | GC |

**Table 4: IGMP Filtering and Throttling Commands (Continued)**

| Command | Function | Mode |
|---|---|---|
| permit, deny | Sets a profile access mode to permit or deny | IPC |
| range | Specifies one or a range of multicast addresses for a profile | IPC |
| ip igmp filter | Assigns an IGMP filter profile to an interface | IC |
| ip igmp max-groups | Specifies an IGMP throttling number for an interface | IC |
| ip igmp max-groups action | Sets the IGMP throttling action for an interface | IC |
| ip igmp query-drop | Drops any received IGMP query packets | IC |
| ip multicast-data-drop | Drops all multicast data packets | IC |
| show ip igmp filter | Displays the IGMP filtering status | PE |
| show ip igmp profile | Displays IGMP profiles and settings | PE |
| show ip igmp query-drop | Shows if the interface is configured to drop IGMP query packets | PE |
| show ip igmp throttle interface | Displays the IGMP throttling setting for interfaces | PE |
| show ip multicast-data-drop | Shows if the interface is configured to drop multicast data packets | PE |

## **ip igmp filter** (Global Configuration)

This command globally enables IGMP filtering and throttling on the switch. Use the **no** form to disable the feature.

### SYNTAX

[**no**] **ip igmp filter**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- IGMP filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. An IGMP filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, IGMP join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the IGMP join report is forwarded as normal. If a requested multicast group is denied, the IGMP join report is dropped.

- IGMP filtering and throttling only applies to dynamically learned multicast groups, it does not apply to statically configured groups.

- The IGMP filtering feature operates in the same manner when MVR is used to forward multicast traffic.

#### EXAMPLE

```
Console(config)#ip igmp filter
Console(config)#
```

## ip igmp profile

This command creates an IGMP filter profile number and enters IGMP profile configuration mode. Use the **no** form to delete a profile number.

#### SYNTAX

[**no**] **ip igmp profile** *profile-number*

*profile-number* - An IGMP filter profile number. (Range: 1-4294967295)

#### DEFAULT SETTING

Disabled

#### COMMAND MODE

Global Configuration

#### COMMAND USAGE

A profile defines the multicast groups that a subscriber is permitted or denied to join. The same profile can be applied to many interfaces, but only one profile can be assigned to one interface. Each profile has only one access mode; either permit or deny.

#### EXAMPLE

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#
```

## permit, deny

This command sets the access mode for an IGMP filter profile. Use the **no** form to delete a profile number.

#### SYNTAX

{**permit** | **deny**}

#### DEFAULT SETTING

Deny

#### COMMAND MODE

IGMP Profile Configuration

#### COMMAND USAGE

- Each profile has only one access mode; either permit or deny.
- When the access mode is set to permit, IGMP join reports are processed when a multicast group falls within the controlled range. When the access mode is set to

deny, IGMP join reports are only processed when a multicast group is not in the controlled range.

### Example

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#permit
Console(config-igmp-profile)#
```

## range

This command specifies multicast group addresses for a profile. Use the **no** form to delete addresses from a profile.

### Syntax

[**no**] **range** *low-ip-address* [*high-ip-address*]

*low-ip-address* - A valid IP address of a multicast group or start of a group range.

*high-ip-address* - A valid IP address for the end of a multicast group range.

### Default Setting

None

### Command Mode

IGMP Profile Configuration

### Command Usage

Enter this command multiple times to specify more than one multicast address or address range for a profile.

### Example

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#range 239.1.1.1
Console(config-igmp-profile)#range 239.2.3.1 239.2.3.100
Console(config-igmp-profile)#
```

## ip igmp filter (Interface Configuration)

This command assigns an IGMP filtering profile to an interface on the switch. Use the **no** form to remove a profile from an interface.

### Syntax

[**no**] **ip igmp filter** *profile-number*

*profile-number* - An IGMP filter profile number. (Range: 1-4294967295)

### Default Setting

None

### COMMAND MODE
Interface Configuration

### COMMAND USAGE
- The IGMP filtering profile must first be created with the ip igmp profile command before being able to assign it to an interface.
- Only one profile can be assigned to an interface.
- A profile can also be assigned to a trunk interface. When ports are configured as trunk members, the trunk uses the filtering profile assigned to the first port member in the trunk.

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp filter 19
Console(config-if)#
```

## ip igmp max-groups

This command sets the IGMP throttling number for an interface on the switch. Use the **no** form to restore the default setting.

### SYNTAX

**ip igmp max-groups** *number*

**no ip igmp max-groups**

*number* - The maximum number of multicast groups an interface can join at the same time. (Range: 0-64)

### DEFAULT SETTING
64

### COMMAND MODE
Interface Configuration (Ethernet)

### COMMAND USAGE
- IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.
- IGMP throttling can also be set on a trunk interface. When ports are configured as trunk members, the trunk uses the throttling settings of the first port member in the trunk.

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups 10
Console(config-if)#
```

## ip igmp max-groups action

This command sets the IGMP throttling action for an interface on the switch.

### SYNTAX

**ip igmp max-groups action** {**replace** | **deny**}

**replace** - The new multicast group replaces an existing group.

**deny** - The new multicast group join report is dropped.

### DEFAULT SETTING

Deny

### COMMAND MODE

Interface Configuration (Ethernet)

### COMMAND USAGE

When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups action replace
Console(config-if)#
```

## ip igmp query-drop

This command drops any received IGMP query packets. Use the no form to restore the default setting.

### SYNTAX

[**no**] **ip igmp query-drop**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Interface Configuration (Ethernet)

### COMMAND USAGE

This command can be used to drop any query packets received on the specified interface. If this switch is acting as a Querier, this prevents it from being affected by messages received from another Querier.

#### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp query-drop
Console(config-if)#
```

## ip multicast-data-drop

This command drops all multicast data packets

#### SYNTAX

[**no**] **ip multicast-data-drop**

#### DEFAULT SETTING

Disabled

#### COMMAND MODE

Interface Configuration (Ethernet)

#### COMMAND USAGE

This command can be used to stop multicast services from being forwarded to users attached to the downstream port (i.e., the interfaces specified by this command).

#### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip multicast-data-drop
Console(config-if)#
```

## show ip igmp filter

This command displays the global and interface settings for IGMP filtering.

#### SYNTAX

**show ip igmp filter** [**interface** *interface*]

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

#### DEFAULT SETTING

None

#### COMMAND MODE

Privileged Exec

#### EXAMPLE

```
Console#show ip igmp filter
IGMP filter enabled
```

```
Console#show ip igmp filter interface ethernet 1/1
Ethernet 1/1 information
---------------------------------
 IGMP Profile 19
  Deny
  range 239.1.1.1 239.1.1.1
  range 239.2.3.1 239.2.3.100
Console#
```

## show ip igmp profile

This command displays IGMP filtering profiles created on the switch.

### SYNTAX

**show ip igmp profile** [*profile-number*

*profile-number* - An existing IGMP filter profile number. (Range: 1-4294967295)

### DEFAULT SETTING

None

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show ip igmp profile
IGMP Profile 19
IGMP Profile 50
Console#show ip igmp profile 19
IGMP Profile 19
  Deny
  range 239.1.1.1 239.1.1.1
  range 239.2.3.1 239.2.3.100
Console#
```

## show ip igmp query-drop

This command shows if the specified interface is configured to drop IGMP query packets.

### SYNTAX

**show ip igmp throttle interface** [*interface*]

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

### DEFAULT SETTING

None

#### COMMAND MODE
Privileged Exec

#### COMMAND USAGE
Using this command without specifying an interface displays all interfaces.

#### EXAMPLE

```
Console#show ip igmp query-drop interface ethernet 1/1
Ethernet 1/1: Enabled
Console#
```

### show ip igmp throttle interface

This command displays the interface settings for IGMP throttling.

#### SYNTAX

**show ip igmp throttle interface** [*interface*]

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

#### DEFAULT SETTING
None

#### COMMAND MODE
Privileged Exec

#### COMMAND USAGE
Using this command without specifying an interface displays all interfaces.

#### EXAMPLE

```
Console#show ip igmp throttle interface ethernet 1/1
Eth  1/1 Information
  Status : TRUE
  Action : Deny
  Max Multicast Groups : 32
  Current Multicast Groups : 0

Console#
```

### show ip multicast-data-drop

This command shows if the specified interface is configured to drop multicast data packets.

#### SYNTAX

**show ip igmp throttle interface** [*interface*]

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

### DEFAULT SETTING
None

### COMMAND MODE
Privileged Exec

### COMMAND USAGE
Using this command without specifying an interface displays all interfaces.

### EXAMPLE

```
Console#show ip multicast-data-drop interface ethernet 1/1
Ethernet 1/1: Enabled
Console#
```

## MULTICAST VLAN REGISTRATION

This section describes commands used to configure Multicast VLAN Registration (MVR). A single network-wide VLAN can be used to transmit multicast traffic (such as television channels) across a service provider's network. Any multicast traffic entering an MVR VLAN is sent to all subscribers. This can significantly reduce to processing overhead required to dynamically monitor and establish the distribution tree for a normal multicast VLAN. Also note that MVR maintains the user isolation and data security provided by VLAN segregation by passing only multicast traffic into other VLANs to which the subscribers belong.

**Table 5: Multicast VLAN Registration Commands**

| Command | Function | Mode |
|---|---|---|
| mvr | Globally enables MVR, statically configures MVR group address(es), or specifies the MVR VLAN identifier | GC |
| mvr upstream-source-ip | Configures the source IP address assigned to all control packets sent upstream | GC |
| mvr immediate-leave | Enables immediate leave capability | IC |
| mvr type | Configures an interface as an MVR receiver or source port | IC |
| mvr vlan group | Configures an interface as a static member of an MVR group which is forwarded from the MVR VLAN to the specified interface within the receiver VLAN | IC |
| show mvr | Shows information about the global MVR configuration settings, interfaces attached to the MVR VLAN, or the multicast groups assigned to the MVR VLAN | PE |

**mvr** This command enables Multicast VLAN Registration (MVR) globally on the switch, statically configures MVR multicast group IP address(es) using the **group** keyword, or specifies the MVR VLAN identifier using the **vlan** keyword. Use the **no** form of this command without any keywords to globally disable MVR. Use the **no** form with the **group** keyword to remove a specific address or range of addresses. Or use the **no** form with the **vlan** keyword to restore the default MVR VLAN.

### SYNTAX

[**no**] **mvr** [**group** *ip-address* [*count*] | **vlan** *vlan-id*]

**group** - Defines a multicast service sent to all attached subscribers.

*ip-address* - IP address for an MVR multicast group.
(Range: 224.0.1.0 - 239.255.255.255)

*count* - The number of contiguous MVR group addresses. (Range: 1-255)

**vlan** - Specifies the VLAN through which MVR multicast data is received. This is also the VLAN to which all source ports must be assigned.

*vlan-id* - MVR VLAN ID (Range: 1-4093)

### DEFAULT SETTING

MVR is disabled.
No MVR group address is defined.
The default number of contiguous addresses is 0.
MVR VLAN ID is 1.

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- Use the **mvr group** command to statically configure all multicast group addresses that will join the MVR VLAN. Any multicast data associated an MVR group is sent from all source ports, and to all receiver ports that have registered to receive data from that multicast group.

- The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.

- MVR source ports can be configured as members of the MVR VLAN using the switchport allowed vlan command and switchport native vlan command, but MVR receiver ports should not be statically configured as members of this VLAN.

- IGMP snooping must be enabled to a allow a subscriber to dynamically join or leave an MVR group (see the ip igmp snooping command). Note that only IGMP version 2 or 3 hosts can issue multicast join or leave messages.

- IGMP snooping and MVR share a maximum number of 255 groups. Any multicast streams received in excess of this limitation will be flooded to all ports in the associated VLAN.

### EXAMPLE

The following example enables MVR globally, and configures a range of MVR group addresses:

```
Console(config)#mvr
Console(config)#mvr group 228.1.23.1 10
Console(config)#
```

## mvr upstream-source-ip

This command configures the source IP address assigned to all MVR control packets sent upstream. Use the **no** form to restore the default setting.

### SYNTAX

**mvr upstream-source-ip** *source-ip-address*

**no mvr upstream-source-ip**

*source-ip-address* – The source IP address assigned to all MVR control packets sent upstream.

### DEFAULT SETTING

All MVR reports sent upstream use a null source IP address

### COMMAND MODE

Global Configuration

### EXAMPLE

```
Console(config)#mvr upstream-source-ip 192.168.0.3
Console(config)#
```

## mvr immediate-leave

This command causes the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group. Use the **no** form to restore the default settings.

### SYNTAX

[**no**] **mvr immediate**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE

- Immediate leave applies only to receiver ports. When enabled, the receiver port is immediately removed from the multicast group identified in the leave message. When immediate leave is disabled, the switch follows the standard rules by sending a group-specific query to the receiver port and waiting for a response to determine if there are any remaining subscribers for that multicast group before removing the port from the group list.

- Using immediate leave can speed up leave latency, but should only be enabled on a port attached to one multicast subscriber to avoid disrupting services to other group members attached to the same interface.

- Immediate leave does not apply to multicast groups which have been statically assigned to a port.

### EXAMPLE
The following enables immediate leave on a receiver port.

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr immediate
Console(config-if)#
```

## mvr type

This command configures an interface as an MVR receiver or source port. Use the **no** form to restore the default settings.

### SYNTAX

[**no**] **mvr type** {**receiver** | **source**}

**receiver** - Configures the interface as a subscriber port that can receive multicast data.

**source** - Configures the interface as an uplink port that can send and receive multicast data for the configured multicast groups.

### DEFAULT SETTING
The port type is not defined.

### COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE
- A port which is not configured as an MVR receiver or source port can use IGMP snooping to join or leave multicast groups using the standard rules for multicast filtering.

- Receiver ports can belong to different VLANs, but should not be configured as a member of the MVR VLAN. IGMP snooping can be used to allow a receiver port to dynamically join or leave multicast groups sourced through the MVR VLAN. Also, note that VLAN membership for MVR receiver ports cannot be set to trunk mode (see the switchport mode command).

- One or more interfaces may be configured as MVR source ports. A source port is able to both receive and send data for multicast groups which it has joined through IGMP snooping or which have been assigned through the mvr group (Global Configuration) command.

- IGMP snooping must be enabled to a allow a subscriber to dynamically join or leave an MVR group (see the ip igmp snooping command). Note that only IGMP version 2 or 3 hosts can issue multicast join or leave messages.

#### EXAMPLE

The following configures one source port and several receiver ports on the switch.

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr type source
Console(config-if)#exit
Console(config)#interface ethernet 1/6
Console(config-if)#mvr type receiver
Console(config-if)#exit
Console(config)#interface ethernet 1/7
Console(config-if)#mvr type receiver
Console(config-if)#
```

## mvr vlan group

This command statically binds a multicast group to a port which will receive long-term multicast streams associated with a stable set of hosts. Use the **no** form to restore the default settings.

#### SYNTAX

[**no**] **mvr vlan** *vlan-id* **group** *ip-address*

*vlan-id* - Receiver VLAN to which the specified multicast traffic is flooded. (Range: 1-4093)

**group** - Defines a multicast service sent to the selected port.

*ip-address* - Statically configures an interface to receive multicast traffic from the IP address specified for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

#### DEFAULT SETTING

No receiver port is a member of any configured multicast group.

#### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

#### COMMAND USAGE

- Multicast groups can be statically assigned to a receiver port using this command.
- The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.
- IGMP snooping must be enabled to a allow a subscriber to dynamically join or leave an MVR group (see the ip igmp snooping command). Note that only IGMP version 2 or 3 hosts can issue multicast join or leave messages.

### EXAMPLE

The following statically assigns a multicast group to a receiver port:

```
Console(config)#interface ethernet 1/7
Console(config-if)#mvr type receiver
Console(config-if)#mvr vlan 3 group 225.0.0.5
Console(config-if)#
```

## show mvr

This command shows information about the global MVR configuration settings when entered without any keywords, the interfaces attached to the MVR VLAN using the **interface** keyword, or the multicast groups assigned to the MVR VLAN using the **members** keyword.

### SYNTAX

**show mvr** [**interface** [*interface*] | **members** [*ip-address*]]

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

*ip-address* - IP address for an MVR multicast group.
(Range: 224.0.1.0 - 239.255.255.255)

### DEFAULT SETTING

Displays global configuration settings for MVR when no keywords are used.

### COMMAND MODE

Privileged Exec

### COMMAND USAGE

Enter this command without any keywords to display the global settings for MVR. Use the **interface** keyword to display information about interfaces attached to the MVR VLAN. Or use the **members** keyword to display information about multicast groups assigned to the MVR VLAN.

### EXAMPLE

The following shows the global MVR settings:

```
Console#show mvr
 MVR Config Status          : Enabled
 MVR Running Status         : Active
 MVR Multicast VLAN         : 1
 MVR Current Groups         : 10
 MVR Max. Supported Groups : 255
 MVR Upstream Source IP     : 192.168.0.3
Console#
```

**Table 6: show mvr** - display description

| Field | Description |
|---|---|
| MVR Config Status | Shows if MVR is globally enabled on the switch. |
| MVR Running Status | Indicates whether or not all necessary conditions in the MVR environment are satisfied. (Running status is true as long as MVR Status is enabled, and the specified MVR VLAN exists.) |
| MVR Multicast VLAN | Shows the VLAN used to transport all MVR multicast traffic. |
| MVR Current Groups | The current number of MVR group addresses. |
| MVR Max. Supported Groups | The maximum number of supported MVR group addresses. |
| MVR Upstream Source IP | The source IP address assigned to all upstream control packets. |

The following displays information about the interfaces attached to the MVR VLAN:

```
Console#show mvr interface
 Port      Type       Status        Immediate   Static Group Address
 --------  --------   ------------- ---------   -------------------
 Eth1/ 2   Source     Active/Up
 Eth1/ 3   Source     Inactive/Down
 Eth1/ 1   Receiver   Active/Up     Disabled    225.0.0.1(VLAN1)
                                    225.0.0.9(VLAN3)
 Eth1/ 4   Receiver   Active/Down   Disabled

Console#
```

**Table 7: show mvr interface** - display description

| Field | Description |
|---|---|
| Port | Shows interfaces attached to the MVR. |
| Type | Shows the MVR port type. |
| Status | Shows the MVR status and interface status. MVR status for source ports is “ACTIVE” if MVR is globally enabled on the switch. MVR status for receiver ports is “ACTIVE” only if there are subscribers receiving multicast traffic from one of the MVR groups, or a multicast group has been statically assigned to an interface. |
| Immediate Leave | Shows if immediate leave is enabled or disabled. |
| Static Group Address | Shows any static MVR group assigned to an interface, and the receiver VLAN. |

The following shows information about the interfaces associated with multicast groups assigned to the MVR VLAN:

```
Console#show mvr members
 MVR Forwarding Entry Count:1
 Group Address    Source Address   VLAN  Forwarding Port
 -------------    --------------   ----  --------------
 225.0.0.9        *                2     Eth1/ 1(VLAN3)   Eth1/ 2(VLAN2)
Console#
```

**Table 8: show mvr members** - display description

| Field | Description |
|---|---|
| MVR Forwarding Entry Count | The number of multicast services currently being forwarded from the MVR VLAN. |
| Group Address | Multicast groups assigned to the MVR VLAN. |
| Source Address | Indicates the source address of the multicast service, or displays an asterisk if the group address has been statically assigned. |
| VLAN | Indicates the MVR VLAN receiving the multicast service. |
| Forwarding Port | Shows the interfaces with subscribers for multicast services provided through the MVR VLAN. Also shows the VLAN through which the service is received. Note that this may be different from the MVR VLAN if the group address has been statically assigned. |

## IGMP (LAYER 3)

This section describes commands used to configure Layer 3 Internet Group Management Protocol (IGMP) on the switch.

**Table 9: IGMP Commands** (Layer 3)

| Command | Function | Mode |
|---|---|---|
| ip igmp | Enables IGMP for the specified interface | IC |
| ip igmp last-member-query-interval | Configures the frequency at which to send query messages in response to receiving a leave message | IC |
| ip igmp max-resp-interval | Configures the maximum host response time | IC |
| ip igmp query-interval | Configures frequency for sending host query messages | IC |
| ip igmp robustval | Configures the expected packet loss | IC |
| ip igmp static-group | Configures the router to be a static member of a multicast group on the specified VLAN interface | IC |
| ip igmp version | Configures IGMP version used on this interface | IC |
| clear ip igmp group | Deletes entries from the IGMP cache | PE |
| show ip igmp groups | Displays information for IGMP groups | PE |
| show ip igmp interface | Displays multicast information for the specified interface | PE |

### ip igmp

This command enables IGMP on a VLAN interface. Use the **no** form of this command to disable IGMP on the specified interface.

#### SYNTAX

[**no**] **ip igmp**

#### DEFAULT SETTING

Disabled

#### COMMAND MODE

Interface Configuration (VLAN)

#### COMMAND USAGE

- IGMP (including query functions) can be enabled for specific VLAN interfaces at Layer 3 through the **ip igmp** command.
- When a multicast routing protocol, such as PIM - Dense Mode, is enabled, IGMP is also enabled.

#### EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip igmp
Console(config-if)#end
Console#show ip igmp interface
 IGMP                          : Enabled
 IGMP Version                  : 2
 IGMP Proxy                    : Disabled
 IGMP Unsolicited-report-interval : 400 sec
 Robustness variable           : 2
 Query Interval                : 125 sec
 Query Max Response Time       : 100 (resolution in 0.1 sec)
 Last Member Query Interval    : 10  (resolution in 0.1 sec)
 Querier                       : 0.0.0.0
 Joined Groups :
 Static Groups :

Console#
```

#### RELATED COMMANDS

ip igmp snooping (958)
show ip igmp snooping (972)

### ip igmp last-member-query-interval

This command configures the frequency at which to send IGMP group-specific or IGMPv3 group-source-specific query messages in response to receiving a group-specific or group-source-specific leave message. Use the **no** form to restore the default setting.

#### SYNTAX

**ip igmp last-member-query-interval** *seconds*

**no ip igmp last-member-query-interval**

*seconds* - The frequency at which the switch sends group-specific or group-source-specific queries upon receipt of a leave message. (Range: 1-255 tenths of a second)

#### DEFAULT SETTING

10 (1 second)

#### COMMAND MODE

Interface Configuration (VLAN)

#### COMMAND USAGE

When the switch receives an IGMPv2 or IGMPv3 leave message from a host that wants to leave a multicast group, source or channel, it sends a number of group-specific or group-source-specific query messages at intervals defined by this command. If no response is received after this period, the switch stops forwarding for the group, source or channel.

**EXAMPLE**

```
Console(config)#interface vlan 1
Console(config-if)#ip igmp last-member-query-interval 20
Console(config-if)#
```

## ip igmp max-resp-interval

This command configures the maximum response time advertised in IGMP queries. Use the **no** form of this command to restore the default.

**SYNTAX**

**ip igmp max-resp-interval** *seconds*

**no ip igmp max-resp-interval**

*seconds* - The report delay advertised in IGMP queries. (Range: 0-255 tenths of a second)

**DEFAULT SETTING**

100 (10 seconds)

**COMMAND MODE**

Interface Configuration (VLAN)

**COMMAND USAGE**

- IGMPv1 does not support a configurable maximum response time for query messages. It is fixed at 10 seconds for IGMPv1.
- By varying the Maximum Response Interval, the burstiness of IGMP messages passed on the subnet can be tuned; where larger values make the traffic less bursty, as host responses are spread out over a larger interval.
- The number of seconds represented by the maximum response interval must be less than the Query Interval (page 994).

**EXAMPLE**

The following shows how to configure the maximum response time to 20 seconds.

```
Console(config-if)#ip igmp query-max-response-time 200
Console(config-if)#
```

**RELATED COMMANDS**

ip igmp version (996)
ip igmp query-interval (994)

## ip igmp query-interval

This command configures the frequency at which host query messages are sent. Use the **no** form to restore the default.

### SYNTAX

**ip igmp query-interval** *seconds*

**no ip igmp query-interval**

*seconds* - The frequency at which the switch sends IGMP host-query messages. (Range: 1-255 seconds)

### DEFAULT SETTING

125 seconds

### COMMAND MODE

Interface Configuration (VLAN)

### COMMAND USAGE

- Multicast routers send host query messages to determine the interfaces that are connected to downstream hosts requesting a specific multicast service. Only the designated multicast router for a subnet sends host query messages, which are addressed to the multicast address 224.0.0.1, and uses a time-to-live (TTL) value of 1.
- For IGMP Version 1, the designated router is elected according to the multicast routing protocol that runs on the LAN. But for IGMP Version 2 and 3, the designated querier is the lowest IP-addressed multicast router on the subnet.

### EXAMPLE

The following shows how to configure the query interval to 100 seconds.

```
Console(config-if)#ip igmp query-interval 100
Console(config-if)#
```

### RELATED COMMANDS

ip igmp max-resp-interval (993)

## ip igmp robustval

This command specifies the robustness (expected packet loss) for this interface. Use the **no** form of this command to restore the default value.

### SYNTAX

**ip igmp robustval** *robust-value*

**no ip igmp robustval**

*robust-value* - The robustness of this interface. (Range: 1-255)

### DEFAULT SETTING

2

#### COMMAND MODE
Interface Configuration (VLAN)

#### COMMAND USAGE
- The robustness value is used in calculating the appropriate range for other IGMP variables, such as the Group Membership Interval, as well as the Other Querier Present Interval, and the Startup Query Count (RFC 3376).

- Routers adopt the robustness value from the most recently received query. If the querier's robustness variable (QRV) is zero, indicating that the QRV field does not contain a declared robustness value, the switch will set the robustness variable to the value statically configured by this command. If the QRV exceeds 7, the maximum value of the QRV field, the robustness value is set to zero, meaning that this device will not advertise a QRV in any query messages it subsequently sends.

#### EXAMPLE
```
Console(config-if)#ip igmp robustness-variable 3
Console(config-if)#
```

### ip igmp static-group

This command configures the router to be a static member of a multicast group on the specified VLAN interface. Use the **no** form to remove the static mapping.

#### SYNTAX

**ip igmp static-group** *group-address* [**source** *source-address*]

**no ip igmp static-group**

*group-address* - IP multicast group address. (The group addresses specified cannot be in the range of 224.0.0.1 - 239.255.255.255.)

*source-address* - Source address for a multicast server transmitting traffic to the corresponding multicast group address.

#### DEFAULT SETTING
None

#### COMMAND MODE
Interface Configuration (VLAN)

#### COMMAND USAGE
- Group addresses within the entire multicast group address range can be specified with this command. However, if any address within the source-specific multicast (SSM) address range (default 232/8) is specified, but no source address is included in the command, the request to join the multicast group will fail unless the next node up the reverse path tree has statically mapped this group to a specific source address. Also, if an address outside of the SSM address range is specified, and a specific source address is included in the command, the request to join the multicast group will also fail if the next node up the reverse path tree has enabled the PIM-SSM protocol.

- If a static group is configured for an any-source multicast (*,G), a source address cannot subsequently be defined for this group without first deleting the entry.
- If a static group is configured for one or more source-specific multicasts (S,G), an any-source multicast (*,G) cannot subsequently be defined for this group without first deleting all of the associated (S,G) entries.
- Using the **no** form of this command to delete a static group without specifying the source address will delete all any-source and source-specific multicast entries for the specified group.
- The switch supports a maximum of 16 static group entries.

### EXAMPLE

The following example assigns VLAN 1 as a static member of the specified multicast group.

```
Console(config)#interface vlan1
Console(config-if)#ip igmp static-group 225.1.1.1
```

## ip igmp version

This command configures the IGMP version used on an interface. Use the **no** form of this command to restore the default.

### SYNTAX

**ip igmp version** {**1** | **2** | **3**}

**no ip igmp version**

**1** - IGMP Version 1

**2** - IGMP Version 2

**3** - IGMP Version 3

### DEFAULT SETTING

IGMP Version 2

### COMMAND MODE

Interface Configuration (VLAN)

### COMMAND USAGE

- All routers on the subnet must support the same version. However, the multicast hosts on the subnet may support any of the IGMP versions 1 - 3.
- If the switch receives an IGMP Version 1 Membership Report, it sets a timer to note that there are Version 1 hosts which are members of the group for which it heard the report.

  If there are Version 1 hosts present for a particular group, the switch will ignore any Leave Group messages that it receives for that group.

#### EXAMPLE

```
Console(config-if)#ip igmp version 1
Console(config-if)#
```

## clear ip igmp group

This command deletes entries from the IGMP cache.

#### SYNTAX

**clear ip igmp group** [*group-address* | **interface** *interface*]

*group-address* - IP address of the multicast group.

*interface*

**vlan** *vlan-id* - VLAN ID. (Range: 1-4093)

#### DEFAULT SETTING

Deletes all entries in the cache if no options are selected.

#### COMMAND MODE

Privileged Exec

#### COMMAND USAGE

Enter the address for a multicast group to delete all entries for the specified group. Enter the interface option to delete all multicast groups for the specified interface. Enter no options to clear all multicast groups from the cache.

#### EXAMPLE

The following example clears all multicast group entries for VLAN 1.

```
Console#clear ip igmp interface vlan1
Console#
```

## show ip igmp groups

This command displays information on multicast groups active on the switch and learned through IGMP.

#### SYNTAX

**show ip igmp groups** [{*group-address* | *interface*} [**detail**] | **detail**]

*group-address* - IP multicast group address.

*interface*

**vlan** *vlan-id* - VLAN ID. (Range: 1-4093)

**detail** - Displays detailed information about the multicast process and source addresses when available.

#### COMMAND MODE

Privileged Exec

### COMMAND USAGE

To display information about multicast groups, IGMP must first be enabled on the interface to which a group has been assigned using the ip igmp command, and multicast routing must be enabled globally on the system using the ip multicast-routing command.

### EXAMPLE

The following shows options for displaying IGMP group information by interface, group address, and static listing.

```
Console#show ip igmp groups
GroupAddress   InterfaceVlan  Lastreporter   Uptime  Expire  V1Timer
--------------- --------------- --------------- -------- -------- --------
   224.0.17.17             1    192.168.1.10    0:0:1   0:4:19    0:0:0
Console#show ip igmp groups 234.5.6.8
GroupAddress   InterfaceVlan  Lastreporter   Uptime  Expire  V1Timer
--------------- --------------- --------------- -------- -------- --------
   224.0.17.17             1    192.168.1.10    0:0:1   0:4:19    0:0:0
Console#show ip igmp groups interface vlan 1
GroupAddress   VLAN  LastReporter   Uptime  Expire  V1 Timer
--------------- ------ --------------- -------- -------- --------
   224.0.17.17     1    192.168.1.10    0:0:1   0:4:19    0:0:0
Console#
```

**Table 10: show ip igmp groups** - display description

| Field | Description |
|---|---|
| Group Address | IP multicast group address with subscribers directly attached or downstream from the switch. |
| VLAN | The interface on the switch that has received traffic directed to the multicast group address. |
| Last Reporter | The IP address of the source of the last membership report received for this multicast group address on this interface. |
| Uptime | The time elapsed since this entry was created. |
| Expire | The time remaining before this entry will be aged out. (The default is 260 seconds.)<br>This field displays “stopped” if the Group Mode is INCLUDE. |
| V1 Timer | The time remaining until the switch assumes that there are no longer any IGMP Version 1 members on the IP subnet attached to this interface.<br>◆ If the switch receives an IGMP Version 1 Membership Report, it sets a timer to note that there are Version 1 hosts present which are members of the group for which it heard the report.<br>◆ If there are Version 1 hosts present for a particular group, the switch will ignore any Leave Group messages that it receives for that group. |

The following shows the information displayed in a detailed listing for a dynamically learned multicast group.

```
Console#show ip igmp groups detail
Interface       : vlan 1
Group           : 224.1.2.3
Uptime          : 0h:0m:12s
Group mode      : Include
Last reporter   : 0.0.0.0
```

```
Group Source List:
Source Address  Uptime      v3 Exp      Fwd
--------------- ----------- ----------- ---
      192.1.2.3   0h:0m:12s    0h:0m:0s Yes
Console#
```

**Table 11: show ip igmp groups detail** - display description

| Field | Description |
|---|---|
| Interface | The interface on the switch that has received traffic directed to the multicast group address. |
| Group | IP multicast group address with subscribers directly attached or downstream from the switch, or a static multicast group assigned to this interface. |
| Uptime | The time elapsed since this entry was created. |
| Group mode | In INCLUDE mode, reception of packets sent to the specified multicast address is requested only from those IP source addresses listed in the source-list parameter. In EXCLUDE mode, reception of packets sent to the given multicast address is requested from all IP source addresses except for those listed in the source-list parameter, and where the source timer status has expired. Note that EXCLUDE mode does not apply to SSM addresses. |
| Last Reporter | The IP address of the source of the last membership report received for this multicast group address on this interface. |
| Group Source List | A list of zero or more IP unicast addresses from which multicast reception is desired or not desired, depending on the filter mode. |
| Source Address | The address of one of the multicast servers transmitting traffic to the specified group. |
| Uptime | The time elapsed since this entry was created. |
| v3 Exp | The time remaining before this entry will be aged out. The V3 label indicates that the expire time is only provided for sources learned through IGMP Version 3. (The default is 260 seconds.) |
| Fwd | Indicates whether or not traffic will be forwarded from the multicast source. |

## show ip igmp interface

This command shows multicast information for the specified interface.

### SYNTAX

**show ip igmp interface** [*interface*]

*interface*

vlan *vlan-id* - VLAN ID. (Range: 1-4093)

### DEFAULT SETTING

None

### COMMAND MODE

Privileged Exec

### EXAMPLE

The following example shows the IGMP configuration for VLAN 1, as well as the device currently serving as the IGMP querier for active multicast services on this interface.

```
Console#show ip igmp interface vlan 1
Vlan 1 : up
 IGMP                          : Disabled
 IGMP Version                  : 2
 IGMP Proxy                    : Enabled
 IGMP Unsolicited-report-interval : 400 sec
 Robustness variable           : 2
 Query Interval                : 125 sec
 Query Max Response Time       : 100 (resolution in 0.1 sec)
 Last Member Query Interval    : 10  (resolution in 0.1 sec)
 Querier                       : 0.0.0.0
 Joined Groups :
 Static Groups :
Console#
```

## IGMP PROXY ROUTING

This section describes commands used to configure IGMP Proxy Routing on the switch.

**Table 12: IGMP Proxy Commands**

| Command | Function | Mode |
|---|---|---|
| ip igmp proxy | Enables IGMP proxy service for multicast routing | IC |
| ip igmp proxy unsolicited-report-interval | Specifies how often the upstream interface should transmit unsolicited IGMP reports | IC |
| show ip igmp interface | Displays multicast information for the specified interface | PE |

To enable IGMP proxy service, follow these steps:

1. Use the ip multicast-routing command to enable IP multicasting globally on the router.

2. Use the ip igmp proxy command to enable IGMP proxy on the upstream interface that is attached to an upstream multicast router.

3. Use the ip igmp command to enable IGMP on the downstream interfaces from which to forward IGMP membership reports.

4. Optional – Use the ip igmp proxy unsolicited-report-interval command to indicate how often the system will send unsolicited reports to the upstream router.

## ip igmp proxy

This command enables IGMP proxy service for multicast routing, forwarding IGMP membership information monitored on downstream interfaces onto the upstream interface in a summarized report. Use the **no** form to disable proxy service.

### SYNTAX

[**no**] **ip igmp proxy**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Interface Configuration (VLAN)

### COMMAND USAGE

- When IGMP proxy is enabled on an interface, that interface is known as the upstream or host interface. This interface performs only the host portion of IGMP by sending IGMP membership reports, and automatically disables IGMP router functions.
- Interfaces with IGMP enabled, but not located in the direction of the multicast tree root are known as downstream or router interfaces. These interfaces perform the standard IGMP router functions by maintaining a database of all IGMP subscriptions on the downstream interface. IGMP must therefore be enabled on all downstream interfaces which require proxy multicast service.
- When changes occur in the downstream IGMP groups, a IGMP state change report is created and sent to the upstream router.
- If there is an IGMPv1 or IGMPv2 querier on the upstream network, then the proxy device will act as an IGMPv1 or IGMPv2 host on the upstream interface accordingly. Otherwise, it will act as an IGMPv3 host.
- Multicast routing protocols are not supported on interfaces where IGMP proxy service is enabled.
- Only one upstream interface is supported on the system.
- A maximum of 1024 multicast streams are supported.

### EXAMPLE

The following example enables multicast routing globally on the switch, configures VLAN 2 as a downstream interface, and then VLAN 1 as the upstream interface.

```
Console(config)#ip multicast-routing
Console(config)#interface vlan2
Console(config-if)#ip igmp
Console(config-if)#exit
Console(config)#interface vlan1
Console(config-if)#ip igmp proxy
Console(config-if)#
```

### ip igmp proxy unsolicited-report-interval

This command specifies how often the upstream interface should transmit unsolicited IGMP reports. Use the **no** form to restore the default value.

**SYNTAX**

**ip igmp proxy unsolicited-report-interval** *seconds*

**no ip igmp proxy unsolicited-report-interval**

*seconds* - The interval at which to issue unsolicited reports. (Range: 1-65535 seconds)

**DEFAULT SETTING**
400 seconds

**COMMAND MODE**
Interface Configuration (VLAN)

**EXAMPLE**
The following example sets the interval for sending unsolicited IGMP reports to 5 seconds.

```
Console(config)#interface vlan
Console(config-if)#ip igmp proxy unsolicited-report-interval 5
Console(config)#
```

## MLD (LAYER 3)

This section describes commands used to configure Layer 3 Multicast Listener Discovery (MLD) on the switch.

**Table 13: MLD Commands** (Layer 3)

| Command | Function | Mode |
|---|---|---|
| ipv6 mld | Enables MLD for the specified interface | IC |
| ipv6 mld last-member-query-response-interval | Configures the frequency at which to send query messages in response to receiving a leave message | IC |
| ipv6 mld max-resp-interval | Configures the maximum host response time | IC |
| ipv6 mld query-interval | Configures frequency for sending host query messages | IC |
| ipv6 mld robustval | Configures the expected packet loss | IC |
| ipv6 mld static-group | Statically binds multicast groups to a VLAN interface | IC |
| ipv6 mld version | Configures MLD version used on an interface | IC |
| clear ipv6 mld group | Deletes entries from the MLD cache | PE |
| show ipv6 mld groups | Displays information for MLD groups | PE |
| show ip igmp interface | Displays multicast information for an interface | PE |

## ipv6 mld

This command enables MLD on a VLAN interface. Use the **no** form of this command to disable MLD on the selected interface.

### SYNTAX

[**no**] **ipv6 mld**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Interface Configuration (VLAN)

### COMMAND USAGE

MLD (including query functions) can be enabled for specific VLAN interfaces at Layer 3 through the **ipv6 mld** command.

### EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 mld
Console(config-if)#end
Console#show ipv6 mld interface
Vlan 1 : Up
  MLD                            : Enabled
  MLD Version                    : 2
  MLD Proxy                      : Disabled
  MLD Unsolicited-report-interval : 400 sec
  Robustness variable            : 2
  Query Interval                 : 125 sec
  Query Max Response Time        : 10  sec
  Last Member Query Interval     : 1   sec
  Querier                        : ::
  Joined Groups :
  Static Groups :

Console#
```

## ipv6 mld last-member-query-response-interval

This command configures the frequency at which to send MLD group-specific or MLDv2 group-source-specific query messages in response to receiving a group-specific or group-source-specific leave message from the last known active host on the subnet. Use the **no** form to restore the default setting.

### SYNTAX

**ipv6 mld last-member-query-response-interval** *seconds*

**no ipv6 mld last-member-query-response-interval**

*seconds* - The frequency at which the switch sends group-specific or group-source-specific queries upon receipt of a leave message. (Range: 1-255 seconds)

### DEFAULT SETTING

10 (1 second)

**COMMAND MODE**
Interface Configuration (VLAN)

**COMMAND USAGE**
When the switch receives an MLD or MLDv2 leave message from a host that wants to leave a multicast group, source or channel, it sends a number of group-specific or group-source-specific query messages at intervals defined by this command. If no response is received after this period, the switch stops forwarding for the group, source or channel.

**EXAMPLE**

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 mld last-member-query-response-interval 20
Console(config-if)#
```

## ipv6 mld max-resp-interval

This command configures the maximum response time advertised in MLD queries. Use the **no** form of this command to restore the default setting.

**SYNTAX**

**ipv6 mld max-resp-interval** *seconds*

**no ipv6 mld max-resp-interval**

*seconds* - The report delay advertised in MLD queries. (Range: 0-255 tenths of a second)

**DEFAULT SETTING**
100 (10 seconds)

**COMMAND MODE**
Interface Configuration (VLAN)

**COMMAND USAGE**
- By varying the Maximum Response Interval, the burstiness of MLD messages passed on the subnet can be tuned; where larger values make the traffic less bursty, as host responses are spread out over a larger interval.
- The number of seconds represented by the maximum response interval must be less than the Query Interval (page 1005).

**EXAMPLE**
The following shows how to configure the maximum response time to 20 seconds.

```
Console(config-if)#ipv6 mld max-resp-interval 200
Console(config-if)#
```

**RELATED COMMANDS**
ipv6 mld query-interval (1005)

## ipv6 mld query-interval

This command configures the frequency at which host query messages are sent. Use the **no** form to restore the default.

### SYNTAX

**ipv6 mld query-interval** *seconds*

**no ipv6 mld query-interval**

*seconds* - The frequency at which the switch sends MLD host-query messages. (Range: 1-255 seconds)

### DEFAULT SETTING

125 seconds

### COMMAND MODE

Interface Configuration (VLAN)

### COMMAND USAGE

- Multicast routers send host query messages to determine the interfaces that are connected to downstream hosts requesting a specific multicast service. Only the designated multicast router for a subnet sends host query messages, which are addressed to the link-scope all-nodes multicast address FF02::1, and uses a time-to-live (TTL) value of 1.
- The designated querier is the lowest IP-addressed multicast router on the subnet.

### EXAMPLE

The following shows how to configure the query interval to 100 seconds.

```
Console(config-if)#ipv6 mld query-interval 100
Console(config-if)#
```

### RELATED COMMANDS

ipv6 mld max-resp-interval (1004)

## ipv6 mld robustval

This command specifies the robustness (expected packet loss) for this interface. Use the **no** form of this command to restore the default value.

### SYNTAX

**ipv6 mld robustval** *robust-value*

**no ipv6 mld robustval**

*robust-value* - The robustness of this interface. (Range: 1-255)

### DEFAULT SETTING

2

### COMMAND MODE

Interface Configuration (VLAN)

#### COMMAND USAGE

- The robustness value is used to compensate for expected packet lose on a link. It indicates the number of refresh packets related to the current MLD state which might be lost without having to terminate that state.

- Routers adopt the robustness value from the most recently received query. If the query's robustness variable (QRV) is zero, indicating that the QRV field does not contain a declared robustness value, the switch will set the robustness variable to the value statically configured by this command. If the QRV exceeds 7, the maximum value of the QRV field, the robustness value is set to zero, meaning that this device will not advertise a QRV in any query messages it subsequently sends.

#### EXAMPLE

```
Console(config-if)#ipv6 mld robustval 3
Console(config-if)#
```

### ipv6 mld static-group

This command statically binds multicast groups to a VLAN interface. Use the **no** form to remove the static mapping.

#### SYNTAX

**ipv6 mld static-group** *group-address* [**source** *source-address*]

**no ipv6 mld static-group** [*group-address* [**source** *source-address*]]

*group-address* - IPv6 multicast group address. (Note that link-local scope addresses FF02:* are not allowed.)

*source-address* - IPv6 source address for a multicast server transmitting traffic to the corresponding multicast group address.

#### DEFAULT SETTING

None

#### COMMAND MODE

Interface Configuration (VLAN)

#### COMMAND USAGE

- If a static group is configured for an any-source multicast (*,G), a source address cannot subsequently be defined for this group without first deleting the entry.

- If a static group is configured for one or more source-specific multicasts (S,G), an any-source multicast (*,G) cannot subsequently be defined for this group without first deleting all of the associated (S,G) entries.

- Use the **no** form of this command without specifying a group address to delete all any-source and source-specific multicast entries.

- Use the **no** form of this command to delete a static group without specifying the source address to delete all any-source and source-specific multicast entries for the specified group.

- The switch supports a maximum of 64 static group entries.

**EXAMPLE**

The following example assigns VLAN 1 as a static member of the specified multicast group.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 mld static-group FFEE::0101
Console(config-if)#
```

## ipv6 mld version

This command configures the MLD version used on an interface. Use the **no** form of this command to restore the default setting.

**SYNTAX**

**ipv6 mld version** {**1** | **2**}

**no ipv6 mld version**

**1** - MLD Version 1

**2** - MLD Version 2

**DEFAULT SETTING**

MLD Version 2

**COMMAND MODE**

Interface Configuration (VLAN)

**COMMAND USAGE**

- MLDv1 is derived from IGMPv2, and MLDv2 from IGMPv3. IGMP uses IP Protocol 2 message types, and MLD uses IP Protocol 58 message types, which is a subset of the ICMPv6 messages.
- MLDv2 adds the ability for a node to report interest in listening to packets with a particular multicast address only from specific source addresses as required to support Source-Specific Multicast (SSM), or from all sources except for specific source addresses.
- MLDv2 supports Source-Specific Multicast (SSM) which builds a reverse tree from a host requesting a service back up to the multicast server.
- Multicast hosts on the subnet may support either MLD versions 1 or 2.

**EXAMPLE**

```
Console(config-if)#ipv6 mld version 1
Console(config-if)#
```

## clear ipv6 mld group

This command deletes entries from the MLD cache.

### SYNTAX

**clear ipv6 mld group** [*group-address* | **interface** *interface*]

*group-address* - IPv6 address of the multicast group.

*interface*

**vlan** *vlan-id* - VLAN ID. (Range: 1-4093)

### DEFAULT SETTING

Deletes all entries in the cache if no options are selected.

### COMMAND MODE

Privileged Exec

### COMMAND USAGE

Enter the address for a multicast group to delete all entries for the specified group. Enter the interface option to delete all multicast groups for the specified interface. Enter no options to clear all multicast groups from the cache.

### EXAMPLE

The following example clears all multicast group entries for VLAN 1.

```
Console#clear ipv6 mld interface vlan 1
Console#
```

## show ipv6 mld groups

This command displays information on multicast groups active on the switch and learned through MLD.

### SYNTAX

**show ipv6 mld groups** [{*group-address* | *interface*} [**detail**] | **detail**]

*group-address* - IPv6 multicast group address. (Note that link-local scope addresses FF02:* are not allowed.)

*interface*

**vlan** *vlan-id* - VLAN ID. (Range: 1-4093)

**detail** - Displays detailed information about the multicast process and source addresses when available.

### COMMAND MODE

Privileged Exec

### COMMAND USAGE

To display information about multicast groups, MLD must first be enabled on the interface to which a group has been assigned using the ipv6 mld command, and multicast routing must be enabled globally on the system using the ip multicast-routing command.

### EXAMPLE

The following shows options for displaying MLD group information.

```
Console#show ipv6 mld groups

GroupAddress                          InterfaceVlan   Uptime   Expire
--------------------------------------- --------------- -------- --------
                         FFEE::101             1   0:1:59    Never
Console#show ipv6 mld groups detail
Interface        : VLAN 1
Group            : FFEE::101
Uptime           : 0h:2m:7s
Group Mode       : Include
Last Reporter    : FE80::0101
Group Source List:
Source Address                         Uptime     Expire      Fwd
--------------------------------------- ----------- ----------- ---
                        FFEE::0101 0h:0m:12s   0h:0m:0s    Yes
Console#
```

**Table 14: show ip igmp groups** - display description

| Field | Description |
| --- | --- |
| Group Address | IP multicast group address with subscribers directly attached or downstream from the switch. |
| Interface VLAN | The interface on the switch that has received traffic directed to the multicast group address. |
| Uptime | The time elapsed since this entry was created. |
| Expire | The time remaining before this entry will be aged out. (The default is 260 seconds.)<br>This field displays “stopped” if the Group Mode is INCLUDE. |
| Group Mode | In Include mode, reception of packets sent to the specified multicast address is requested only from those IP source addresses listed in the source-list parameter. In Exclude mode, reception of packets sent to the given multicast address is requested from all IP source addresses except for those listed in the source-list parameter, and where the source timer status has expired. Note that Exclude mode does not apply to SSM addresses. |
| Last Reporter | The IP address of the source of the last membership report received for this multicast group address on this interface. |
| Group Source List | A list of zero or more IP unicast addresses from which multicast reception is desired or not desired, depending on the filter mode. |
| Source Address | The address of one of the multicast servers transmitting traffic to the specified group. |
| Fwd | Indicates whether or not traffic will be forwarded from the multicast source. |

### show ipv6 mld interface

This command shows multicast information for the specified interface.

#### SYNTAX

**show ipv6 mld interface** [*interface*]

*interface*

vlan *vlan-id* - VLAN ID. (Range: 1-4093)

#### DEFAULT SETTING
None

#### COMMAND MODE
Privileged Exec

#### EXAMPLE
The following example shows the MLD configuration for VLAN 1, as well as the device currently serving as the MLD querier for active multicast services on this interface.

```
Console#show ipv6 mld interface vlan 1
Vlan 1 : Up
  MLD                          : Enabled
  MLD Version                  : 2
  MLD Proxy                    : Disabled
  MLD Unsolicited-report-interval : 400 sec
  Robustness variable          : 2
  Query Interval               : 125 sec
  Query Max Response Time      : 10
  Last Member Query Interval   : 1
  Querier                      : FE80::200:E8FF:FE93:82A0
  Joined Groups :
  Static Groups :
    FFEE::101
Console#
```

## MLD PROXY ROUTING

This section describes commands used to configure MLD Proxy Routing on the switch.

**Table 15: IGMP Proxy Commands**

| Command | Function | Mode |
|---|---|---|
| ipv6 mld proxy | Enables MLD proxy service for multicast routing | IC |
| ipv6 mld proxy unsolicited-report-interval | Specifies how often the upstream interface should transmit unsolicited IGMP reports | IC |
| show ipv6 mld interface | Displays multicast information for the specified interface | PE |

To enable MLD proxy service, follow these steps:

1. Use the ipv6 multicast-routing command to enable IP multicasting globally on the router.

2. Use the ipv6 mld proxy command to enable MLD proxy on the upstream interface that is attached to an upstream multicast router.

3. Use the ipv6 mld command to enable MLD on the downstream interfaces from which to forward MLD membership reports.

4. Optional – Use the ipv6 mld proxy unsolicited-report-interval command to indicate how often the system will send unsolicited reports to the upstream router.

## ipv6 mld proxy

This command enables MLD proxy service for multicast routing, forwarding MLD membership information monitored on downstream interfaces onto the upstream interface in a summarized report. Use the **no** form to disable proxy service.

### SYNTAX

[**no**] **ipv6 mld proxy**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Interface Configuration (VLAN)

### COMMAND USAGE

- When MLD proxy is enabled on an interface, that interface is known as the upstream or host interface. This interface performs only the host portion of MLD by sending MLD membership reports, and automatically disables MLD router functions.

- Interfaces with MLD enabled, but not located in the direction of the multicast tree root are known as downstream or router interfaces. These interfaces perform the standard MLD router functions by maintaining a database of all MLD subscriptions on the downstream interface. MLD must therefore be enabled on all downstream interfaces which require proxy multicast service.

- When changes occur in the downstream MLD groups, an MLD state change report is created and sent to the upstream router.

- If there is an MLDv1 querier on the upstream network, then the proxy device will act as an MLDv1 host on the upstream interface accordingly. Otherwise, it will act as an MLDv2 host.

- Multicast routing protocols are not supported on interfaces where MLD proxy service is enabled.

- Only one upstream interface is supported on the system.

- MLD and MLD proxy cannot be enabled on the same interface.
- A maximum of 1024 multicast streams are supported.

**EXAMPLE**
The following example enables multicast routing globally on the switch, configures VLAN 2 as a downstream interface, and then VLAN 1 as the upstream interface.

```
Console(config)#ip multicast-routing
Console(config)#interface vlan2
Console(config-if)#ipv6 mld
Console(config-if)#exit
Console(config)#interface vlan1
Console(config-if)#ipv6 mld proxy
Console(config-if)#
```

## ipv6 mld proxy unsolicited-report-interval

This command specifies how often the upstream interface should transmit unsolicited MLD reports. Use the **no** form to restore the default value.

**SYNTAX**

**ipv6 mld proxy unsolicited-report-interval** *seconds*

**no ipv6 mld proxy unsolicited-report-interval**

*seconds* - The interval at which to issue unsolicited reports. (Range: 1-65535 seconds)

**DEFAULT SETTING**
400 seconds

**COMMAND MODE**
Interface Configuration (VLAN)

**COMMAND USAGE**
- The unsolicited report interval only applies to the interface where MLD proxy has been enabled.
- MLD and MLD proxy cannot be enabled on the same interface.

**EXAMPLE**
The following example sets the interval for sending unsolicited MLD reports to 5 seconds.

```
Console(config)#interface vlan
Console(config-if)#ip igmp proxy unsolicited-report-interval 5
Console(config)#
```

# 43 LLDP COMMANDS

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

**Table 1: LLDP Commands**

| Command | Function | Mode |
|---|---|---|
| lldp | Enables LLDP globally on the switch | GC |
| lldp holdtime-multiplier | Configures the time-to-live (TTL) value sent in LLDP advertisements | GC |
| lldp notification-interval | Configures the allowed interval for sending SNMP notifications about LLDP changes | GC |
| lldp refresh-interval | Configures the periodic transmit interval for LLDP advertisements | GC |
| lldp reinit-delay | Configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down | GC |
| lldp tx-delay | Configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables | GC |
| lldp admin-status | Enables LLDP transmit, receive, or transmit and receive mode on the specified port | IC |
| lldp basic-tlv management-ip-address | Configures an LLDP-enabled port to advertise the management address for this device | IC |
| lldp basic-tlv port-description | Configures an LLDP-enabled port to advertise its port description | IC |
| lldp basic-tlv system-capabilities | Configures an LLDP-enabled port to advertise its system capabilities | IC |
| lldp basic-tlv system-description | Configures an LLDP-enabled port to advertise the system description | IC |
| lldp basic-tlv system-name | Configures an LLDP-enabled port to advertise its system name | IC |
| lldp dot1-tlv proto-ident[1] | Configures an LLDP-enabled port to advertise the supported protocols | IC |
| lldp dot1-tlv proto-vid[1] | Configures an LLDP-enabled port to advertise port related VLAN information | IC |
| lldp dot1-tlv pvid[1] | Configures an LLDP-enabled port to advertise its default VLAN ID | IC |
| lldp dot1-tlv vlan-name[1] | Configures an LLDP-enabled port to advertise its VLAN name | IC |
| lldp dot3-tlv link-agg | Configures an LLDP-enabled port to advertise its link aggregation capabilities | IC |

**Table 1: LLDP Commands (Continued)**

| Command | Function | Mode |
|---|---|---|
| lldp dot3-tlv mac-phy | Configures an LLDP-enabled port to advertise its MAC and physical layer specifications | IC |
| lldp dot3-tlv max-frame | Configures an LLDP-enabled port to advertise its maximum frame size | IC |
| lldp notification | Enables the transmission of SNMP trap notifications about LLDP changes | IC |
| show lldp config | Shows LLDP configuration settings for all ports | PE |
| show lldp info local-device | Shows LLDP global and interface-specific configuration settings for this device | PE |
| show lldp info remote-device | Shows LLDP global and interface-specific configuration settings for remote devices | PE |
| show lldp info statistics | Shows statistical counters for all LLDP-enabled interfaces | PE |

1. Vendor-specific options may or may not be advertised by neighboring devices.

## lldp

This command enables LLDP globally on the switch. Use the **no** form to disable LLDP.

### SYNTAX

[**no**] **lldp**

### DEFAULT SETTING

Enabled

### COMMAND MODE

Global Configuration

### EXAMPLE

```
Console(config)#lldp
Console(config)#
```

## lldp holdtime-multiplier

This command configures the time-to-live (TTL) value sent in LLDP advertisements. Use the **no** form to restore the default setting.

### SYNTAX

**lldp holdtime-multiplier** *value*

**no lldp holdtime-multiplier**

*value* - Calculates the TTL in seconds based on (holdtime-multiplier * refresh-interval) $\leq$ 65536 (Range: 2 - 10)

#### DEFAULT SETTING
Holdtime multiplier: 4
TTL: 4*30 = 120 seconds

#### COMMAND MODE
Global Configuration

#### COMMAND USAGE
The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner.

#### EXAMPLE
```
Console(config)#lldp holdtime-multiplier 10
Console(config)#
```

### lldp notification-interval

This command configures the allowed interval for sending SNMP notifications about LLDP MIB changes. Use the **no** form to restore the default setting.

#### SYNTAX

**lldp notification-interval** *seconds*

**no lldp notification-interval**

*seconds* - Specifies the periodic interval at which SNMP notifications are sent. (Range: 5 - 3600 seconds)

#### DEFAULT SETTING
5 seconds

#### COMMAND MODE
Global Configuration

#### COMMAND USAGE
- This parameter only applies to SNMP applications which use data stored in the LLDP MIB for network monitoring or management.
- Information about changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

#### EXAMPLE
```
Console(config)#lldp notification-interval 30
Console(config)#
```

## lldp refresh-interval

This command configures the periodic transmit interval for LLDP advertisements. Use the **no** form to restore the default setting.

### Syntax

**lldp refresh-interval** *seconds*

**no lldp refresh-delay**

*seconds* - Specifies the periodic interval at which LLDP advertisements are sent. (Range: 5 - 32768 seconds)

### Default Setting

30 seconds

### Command Mode

Global Configuration

### Command Usage

This attribute must comply with the following rule:
(refresh-interval * holdtime-multiplier) ≤ 65536

### Example

```
Console(config)#lldp refresh-interval 60
Console(config)#
```

## lldp reinit-delay

This command configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down. Use the **no** form to restore the default setting.

### Syntax

**lldp reinit-delay** *seconds*

**no lldp reinit-delay**

*seconds* - Specifies the delay before attempting to re-initialize LLDP. (Range: 1 - 10 seconds)

### Default Setting

2 seconds

### Command Mode

Global Configuration

### Command Usage

When LLDP is re-initialized on a port, all information in the remote systems LLDP MIB associated with this port is deleted.

#### EXAMPLE

```
Console(config)#lldp reinit-delay 10
Console(config)#
```

### lldp tx-delay

This command configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables. Use the **no** form to restore the default setting.

#### SYNTAX

**lldp tx-delay** *seconds*

**no lldp tx-delay**

*seconds* - Specifies the transmit delay. (Range: 1 - 8192 seconds)

#### DEFAULT SETTING

2 seconds

#### COMMAND MODE

Global Configuration

#### COMMAND USAGE

- The transmit delay is used to prevent a series of successive LLDP transmissions during a short period of rapid changes in local LLDP MIB objects, and to increase the probability that multiple, rather than single changes, are reported in each transmission.
- This attribute must comply with the following rule:
  (4 * tx-delay) ≤ refresh-interval

#### EXAMPLE

```
Console(config)#lldp tx-delay 10
Console(config)#
```

### lldp admin-status

This command enables LLDP transmit, receive, or transmit and receive mode on the specified port. Use the **no** form to disable this feature.

#### SYNTAX

**lldp admin-status** {**rx-only** | **tx-only** | **tx-rx**}

**no lldp admin-status**

**rx-only** - Only receive LLDP PDUs.

**tx-only** - Only transmit LLDP PDUs.

**tx-rx** - Both transmit and receive LLDP Protocol Data Units (PDUs).

#### DEFAULT SETTING
tx-rx

#### COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

#### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp admin-status rx-only
Console(config-if)#
```

### lldp basic-tlv management-ip-address

This command configures an LLDP-enabled port to advertise the management address for this device. Use the **no** form to disable this feature.

#### SYNTAX

[**no**] **lldp basic-tlv management-ip-address**

#### DEFAULT SETTING
Enabled

#### COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

#### COMMAND USAGE
- The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.
- The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address. The interface number and OID are included to assist SNMP applications to perform network discovery by indicating enterprise specific or other starting points for the search, such as the Interface or Entity MIB.
- Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV.
- Every management address TLV that reports an address that is accessible on a port and protocol VLAN through the particular port should be accompanied by a port and protocol VLAN TLV that indicates the VLAN identifier (VID) associated with the management address reported by this TLV.

#### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv management-ip-address
Console(config-if)#
```

## lldp basic-tlv port-description

This command configures an LLDP-enabled port to advertise its port description. Use the **no** form to disable this feature.

### SYNTAX

[**no**] **lldp basic-tlv port-description**

### DEFAULT SETTING
Enabled

### COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE
The port description is taken from the ifDescr object in RFC 2863, which includes information about the manufacturer, the product name, and the version of the interface hardware/software.

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv port-description
Console(config-if)#
```

## lldp basic-tlv system-capabilities

This command configures an LLDP-enabled port to advertise its system capabilities. Use the **no** form to disable this feature.

### SYNTAX

[**no**] **lldp basic-tlv system-capabilities**

### DEFAULT SETTING
Enabled

### COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE
The system capabilities identifies the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-capabilities
Console(config-if)#
```

## lldp basic-tlv system-description

This command configures an LLDP-enabled port to advertise the system description. Use the **no** form to disable this feature.

### Syntax

[**no**] **lldp basic-tlv system-description**

### Default Setting

Enabled

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

The system description is taken from the sysDescr object in RFC 3418, which includes the full name and version identification of the system's hardware type, software operating system, and networking software.

### Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-description
Console(config-if)#
```

## lldp basic-tlv system-name

This command configures an LLDP-enabled port to advertise the system name. Use the **no** form to disable this feature.

### Syntax

[**no**] **lldp basic-tlv system-name**

### Default Setting

Enabled

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

The system name is taken from the sysName object in RFC 3418, which contains the system's administratively assigned name, and is in turn based on the hostname command.

### Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-name
Console(config-if)#
```

## lldp dot1-tlv proto-ident

This command configures an LLDP-enabled port to advertise the supported protocols. Use the **no** form to disable this feature.

### SYNTAX

[**no**] **lldp dot1-tlv proto-ident**

### DEFAULT SETTING

Enabled

### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE

This option advertises the protocols that are accessible through this interface.

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv proto-ident
Console(config-if)#
```

## lldp dot1-tlv proto-vid

This command configures an LLDP-enabled port to advertise port related VLAN information. Use the **no** form to disable this feature.

### SYNTAX

[**no**] **lldp dot1-tlv proto-vid**

### DEFAULT SETTING

Enabled

### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE

This option advertises the port-based and protocol-based VLANs configured on this interface (see ?$paratext>? on page 892 and ?$paratext>? on page 912).

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv proto-vid
Console(config-if)#
```

## lldp dot1-tlv pvid

This command configures an LLDP-enabled port to advertise its default VLAN ID. Use the **no** form to disable this feature.

### SYNTAX

[**no**] **lldp dot1-tlv pvid**

### DEFAULT SETTING

Enabled

### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE

The port's default VLAN identifier (PVID) indicates the VLAN with which untagged or priority-tagged frames are associated (see the switchport native vlan command).

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv pvid
Console(config-if)#
```

## lldp dot1-tlv vlan-name

This command configures an LLDP-enabled port to advertise its VLAN name. Use the **no** form to disable this feature.

### SYNTAX

[**no**] **lldp dot1-tlv vlan-name**

### DEFAULT SETTING

Enabled

### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE

This option advertises the name of all VLANs to which this interface has been assigned. See ?$paratext>? on page 894 and ?$paratext>? on page 913.

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv vlan-name
Console(config-if)#
```

## lldp dot3-tlv link-agg

This command configures an LLDP-enabled port to advertise link aggregation capabilities. Use the **no** form to disable this feature.

#### SYNTAX

[**no**] **lldp dot3-tlv link-agg**

#### DEFAULT SETTING
Enabled

#### COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

#### COMMAND USAGE
This option advertises link aggregation capabilities, aggregation status of the link, and the 802.3 aggregated port identifier if this interface is currently a link aggregation member.

#### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot3-tlv link-agg
Console(config-if)#
```

### lldp dot3-tlv mac-phy

This command configures an LLDP-enabled port to advertise its MAC and physical layer capabilities. Use the **no** form to disable this feature.

#### SYNTAX

[**no**] **lldp dot3-tlv mac-phy**

#### DEFAULT SETTING
Enabled

#### COMMAND MODE
Interface Configuration (Ethernet, Port Channel)

#### COMMAND USAGE
This option advertises MAC/PHY configuration/status which includes information about auto-negotiation support/capabilities, and operational Multistation Access Unit (MAU) type.

#### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot3-tlv mac-phy
Console(config-if)#
```

### lldp dot3-tlv max-frame

This command configures an LLDP-enabled port to advertise its maximum frame size. Use the **no** form to disable this feature.

### SYNTAX

[**no**] **lldp dot3-tlv max-frame**

### DEFAULT SETTING

Enabled

### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE

Refer to ?$paratext>? on page 622 for information on configuring the maximum frame size for this switch.

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dot3-tlv max-frame
Console(config-if)#
```

## lldp notification

This command enables the transmission of SNMP trap notifications about LLDP changes. Use the **no** form to disable LLDP notifications.

### SYNTAX

[**no**] **lldp notification**

### DEFAULT SETTING

Enabled

### COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

### COMMAND USAGE

- This option sends out SNMP trap notifications to designated target stations at the interval specified by the lldp notification-interval command. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), or organization-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs.

- SNMP trap destinations are defined using the snmp-server host command.

- Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

### EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp notification
Console(config-if)#
```

## show lldp config

This command shows LLDP configuration settings for all ports.

### SYNTAX

**show lldp config** [**detail** *interface*]

**detail** - Shows configuration summary.

interface

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show lldp config

LLDP Global Configuation

 LLDP Enable                : Yes
 LLDP Transmit interval     : 30
 LLDP Hold Time Multiplier  : 4
 LLDP Delay Interval        : 2
 LLDP Reinit Delay          : 2
 LLDP Notification Interval : 5
 LLDP MED fast start counts : 4


LLDP Port Configuration
  Interface |AdminStatus NotificationEnabled
  --------- + ----------- -------------------
  Eth 1/1   | Tx-Rx       True
  Eth 1/2   | Tx-Rx       True
  Eth 1/3   | Tx-Rx       True
  Eth 1/4   | Tx-Rx       True
  Eth 1/5   | Tx-Rx       True
.
.
.
Console#show lldp config detail ethernet 1/1

LLDP Port Configuration Detail

 Port : Eth 1/1
 Admin Status : Tx-Rx
 Notification Enabled : True
 Basic TLVs Advertised:
   port-description
   system-name
   system-description
```

```
  system-capabilities
  management-ip-address
802.1 specific TLVs Advertised:
 *port-vid
 *vlan-name
 *proto-vlan
 *proto-ident
802.3 specific TLVs Advertised:
 *mac-phy
 *poe
 *link-agg
 *max-frame

Console#
```

## show lldp info local-device

This command shows LLDP global and interface-specific configuration settings for this device.

### SYNTAX

**show lldp info local-device** [**detail** *interface*]

**detail** - Shows configuration summary.

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show lldp info local-device

 LLDP Local System Information
  Chassis Type : MAC Address
  Chassis ID   : 00-01-02-03-04-05
  System Name  :
  System Description : EL 326
  System Capabilities Support : Bridge
  System Capabilities Enable  : Bridge
  Management Address : 192.168.0.101 (IPv4)

 LLDP Port Information
 Interface |PortID Type      PortID           PortDesc
 --------- + ---------------- ----------------- ---------------------------
 Eth 1/1   |MAC Address      00-01-02-03-04-06 Ethernet Port on unit 1, port 1
 Eth 1/2   |MAC Address      00-01-02-03-04-07 Ethernet Port on unit 1, port 2
 Eth 1/3   |MAC Address      00-01-02-03-04-08 Ethernet Port on unit 1, port 3
 Eth 1/4   |MAC Address      00-01-02-03-04-09 Ethernet Port on unit 1, port 4
.
.
.
Console#show lldp info local-device detail ethernet 1/1

LLDP Port Information Detail

 Port     : Eth 1/1
```

```
 Port Type : MAC Address
 Port ID   : 00-01-02-03-04-06
 Port Desc : Ethernet Port on unit 1, port 1

Console#
```

## show lldp info remote-device

This command shows LLDP global and interface-specific configuration settings for remote devices attached to an LLDP-enabled port.

### SYNTAX

**show lldp info remote-device** [**detail** *interface*]

**detail** - Shows configuration summary.

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show lldp info remote-device

 LLDP Remote Devices Information

  Interface | ChassisId         PortId            SysName
  --------- + ----------------- ----------------- ---------------------
  Eth 1/1   | 00-01-02-03-04-05 00-01-02-03-04-06

Console#show lldp info remote-device detail ethernet 1/1

 LLDP Remote Devices Information Detail

---------------------------------------------------------------
  Local PortName      : Eth 1/1
  Chassis Type        : MAC Address
  Chassis Id          : 00-01-02-03-04-05
  PortID Type         : MAC Address
  PortID              : 00-01-02-03-04-06
  SysName             :
  System Description : EL 326
  Port Description    : Ethernet Port on unit 1, port 1
  SystemCapSupported : Bridge, Router
  SystemCapEnabled   : Bridge, Router
  Remote Management Address :
    192.168.0.2 (IPv4)
  Remote Port VID : 1
  Remote VLAN Name :
    VLAN-1 : DefaultVlan
  Remote Protocol Identity (Hex) :
    88-CC
  Remote MAC/PHY configuration status :
    Remote port auto-neg supported : Yes
    Remote port auto-neg enabled : Yes
```

```
  Remote port auto-neg advertised cap (Hex) : 6C01
  Remote port MAU type : 30
 Remote Link Aggregation :
  Remote link aggregation capable : Yes
  Remote link aggregation enable : No
 Remote link aggregation port id : 0
 Remote Max Frame Size : 1518

Console#
```

## show lldp info statistics

This command shows statistics based on traffic received through all attached LLDP-enabled interfaces.

### SYNTAX

**show lldp info statistics** [**detail** *interface*]

**detail** - Shows configuration summary.

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show lldp info statistics

 LLDP Device Statistics

  Neighbor Entries List Last Updated : 2450279 seconds
  New Neighbor Entries Count        : 1
  Neighbor Entries Deleted Count    : 0
  Neighbor Entries Dropped Count    : 0
  Neighbor Entries Ageout Count     : 0

  Interface | NumFramesRecvd NumFramesSent NumFramesDiscarded
  --------- + -------------- ------------- ------------------
  Eth 1/1   | 10           11          0
  Eth 1/2   | 0            0           0
  Eth 1/3   | 0            0           0
  Eth 1/4   | 0            0           0
  Eth 1/5   | 0            0           0
:
Console#show lldp info statistics detail ethernet 1/1

 LLDP Port Statistics Detail

  PortName         : Eth 1/1
  Frames Discarded  : 0
  Frames Invalid    : 0
  Frames Received   : 12
  Frames Sent       : 13
  TLVs Unrecognized : 0
  TLVs Discarded    : 0
```

```
  Neighbor Ageouts  : 0
Console#
```

# 44 DOMAIN NAME SERVICE COMMANDS

These commands are used to configure Domain Naming System (DNS) services. Entries can be manually configured in the DNS domain name to IP address mapping table, default domain names configured, or one or more name servers specified to use for domain name to address translation.

Note that domain name services will not be enabled until at least one name server is specified with the ip name-server command and domain lookup is enabled with the ip domain-lookup command.

**Table 1: Address Table Commands**

| Command | Function | Mode |
|---|---|---|
| ip domain-list | Defines a list of default domain names for incomplete host names | GC |
| ip domain-lookup | Enables DNS-based host name-to-address translation | GC |
| ip domain-name | Defines a default domain name for incomplete host names | GC |
| ip host | Creates a static IPv4 host name-to-address mapping | GC |
| ip name-server | Specifies the address of one or more name servers to use for host name-to-address translation | GC |
| ipv6 host | Creates a static IPv6 host name-to-address mapping | GC |
| clear dns cache | Clears all entries from the DNS cache | PE |
| clear host | Deletes entries from the host name-to-address table | PE |
| show dns | Displays the configuration for DNS services | PE |
| show dns cache | Displays entries in the DNS cache | PE |
| show hosts | Displays the static host name-to-address mapping table | PE |

## ip domain-list

This command defines a list of domain names that can be appended to incomplete host names (i.e., host names passed from a client that are not formatted with dotted notation). Use the **no** form to remove a name from this list.

### SYNTAX

[**no**] **ip domain-list** *name*

*name* - Name of the host. Do not include the initial dot that separates the host name from the domain name.
(Range: 1-68 characters)

### DEFAULT SETTING

None

#### COMMAND MODE
Global Configuration

#### COMMAND USAGE
- Domain names are added to the end of the list one at a time.
- When an incomplete host name is received by the DNS service on this switch, it will work through the domain list, appending each domain name in the list to the host name, and checking with the specified name servers for a match.
- If there is no domain list, the domain name specified with the ip domain-name command is used. If there is a domain list, the default domain name is not used.

#### EXAMPLE
This example adds two domain names to the current list and then displays the list.

```
Console(config)#ip domain-list sample.com.jp
Console(config)#ip domain-list sample.com.uk
Console(config)#end
Console#show dns
Domain Lookup Status:
   DNS disabled
Default Domain Name:
   sample.com
Domain Name List:
   sample.com.jp
   sample.com.uk
Name Server List:
Console#
```

#### RELATED COMMANDS
ip domain-name (1033)

## ip domain-lookup

This command enables DNS host name-to-address translation. Use the **no** form to disable DNS.

#### SYNTAX

[**no**] **ip domain-lookup**

#### DEFAULT SETTING
Disabled

#### COMMAND MODE
Global Configuration

#### COMMAND USAGE
- At least one name server must be specified before DNS can be enabled.
- If all name servers are deleted, DNS will automatically be disabled.

### EXAMPLE
This example enables DNS and then displays the configuration.

```
Console(config)#ip domain-lookup
Console(config)#end
Console#show dns
Domain Lookup Status:
  DNS enabled
Default Domain Name:
  sample.com
Domain Name List:
  sample.com.jp
  sample.com.uk
Name Server List:
  192.168.1.55
  10.1.0.55
Console#
```

### RELATED COMMANDS
ip domain-name (1033)
ip name-server (1034)

## ip domain-name

This command defines the default domain name appended to incomplete host names (i.e., host names passed from a client that are not formatted with dotted notation). Use the **no** form to remove the current domain name.

### SYNTAX

**ip domain-name** *name*

**no ip domain-name**

*name* - Name of the host. Do not include the initial dot that separates the host name from the domain name.
(Range: 1-127 characters)

### DEFAULT SETTING
None

### COMMAND MODE
Global Configuration

### EXAMPLE

```
Console(config)#ip domain-name sample.com
Console(config)#end
Console#show dns
Domain Lookup Status:
  DNS Disabled
Default Domain Name:
  sample.com
Domain Name List:
Name Server List:
Console#
```

#### RELATED COMMANDS

ip domain-list (1031)
ip name-server (1034)
ip domain-lookup (1032)

## ip host

This command creates a static entry in the DNS table that maps a host name to an IPv4 address. Use the **no** form to remove an entry.

#### SYNTAX

[**no**] **ip host** *name address*

*name* - Name of an IPv4 host. (Range: 1-100 characters)

*address* - Corresponding IPv4 address.

#### DEFAULT SETTING

No static entries

#### COMMAND MODE

Global Configuration

#### COMMAND USAGE

Use the **no ip host** command to clear static entries, or the clear host command to clear dynamic entries.

#### EXAMPLE

This example maps an IPv4 address to a host name.

```
Console(config)#ip host rd5 192.168.1.55
Console(config)#end
Console#show hosts
No.  Flag Type    IP Address          TTL   Domain
---- ---- ------- ------------------- ----- ------------------------------
   0    2 Address 192.168.1.55              rd5
Console#
```

## ip name-server

This command specifies the address of one or more domain name servers to use for name-to-address resolution. Use the **no** form to remove a name server from this list.

#### SYNTAX

[**no**] **ip name-server** *server-address1* [*server-address2 … server-address6*]

*server-address1* - IP address of domain-name server.

*server-address2 … server-address6* - IP address of additional domain-name servers.

#### DEFAULT SETTING

None

#### COMMAND MODE
Global Configuration

#### COMMAND USAGE
The listed name servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.

#### EXAMPLE
This example adds two domain-name servers to the list and then displays the list.

```
Console(config)#ip name-server 192.168.1.55 10.1.0.55
Console(config)#end
Console#show dns
Domain Lookup Status:
   DNS disabled
Default Domain Name:
   sample.com
Domain Name List:
   sample.com.jp
   sample.com.uk
Name Server List:
   192.168.1.55
   10.1.0.55
Console#
```

#### RELATED COMMANDS
ip domain-name (1033)
ip domain-lookup (1032)

### ipv6 host

This command creates a static entry in the DNS table that maps a host name to an IPv6 address. Use the **no** form to remove an entry.

#### SYNTAX

[**no**] **ipv6 host** *name ipv6-address*

*name* - Name of an IPv6 host. (Range: 1-100 characters)

*ipv6-address* - Corresponding IPv6 address. This address must be entered according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

#### DEFAULT SETTING
No static entries

#### COMMAND MODE
Global Configuration

#### EXAMPLE
This example maps an IPv6 address to a host name.

```
Console(config)#ipv6 host rd6 2001:0db8:1::12
Console(config)#end
Console#show hosts
No.  Flag Type    IP Address           TTL   Domain
---- ---- ------- --------------------  ----- --------------------------------
   0    2 Address 192.168.1.55               rd5
   1    2 Address 2001:DB8:1::12             rd6
Console#
```

## clear dns cache
This command clears all entries in the DNS cache.

#### COMMAND MODE
Privileged Exec

#### EXAMPLE

```
Console#clear dns cache
Console#show dns cache
No.    Flag   Type   IP Address     TTL    Domain
------- ------- ------- -------------- ------- --------
Console#
```

## clear host
This command deletes dynamic entries from the DNS table.

#### SYNTAX
**clear host** {*name* | *}

*name* - Name of the host. (Range: 1-100 characters)

* - Removes all entries.

#### DEFAULT SETTING
None

#### COMMAND MODE
Privileged Exec

#### COMMAND USAGE
Use the **clear host** command to clear dynamic entries, or the no ip host command to clear static entries.

#### EXAMPLE
This example clears all dynamic entries from the DNS table.

```
Console(config)#clear host *
Console(config)#
```

## show dns

This command displays the configuration of the DNS service.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show dns
Domain Lookup Status:
  DNS enabled
Default Domain Name:
  sample.com
Domain Name List:
  sample.com.jp
  sample.com.uk
Name Server List:
  192.168.1.55
  10.1.0.55
Console#
```

## show dns cache

This command displays entries in the DNS cache.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show dns cache
No.     Flag    Type    IP Address      TTL     Domain
------- ------- ------- --------------- ------- --------
      3       4 Host    209.131.36.158      115 www-real.wa1.b.yahoo.com
      4       4 CNAME   POINTER TO:3        115 www.yahoo.com
      5       4 CNAME   POINTER TO:3        115 www.wa1.b.yahoo.com
Console#
```

**Table 2: show dns cache** - display description

| Field | Description |
|---|---|
| No. | The entry number for each resource record. |
| Flag | The flag is always “4” indicating a cache entry and therefore unreliable. |
| Type | This field includes “Host” which specifies the primary name for the owner, and “CNAME” which specifies multiple domain names (or aliases) which are mapped to the same IP address as an existing entry. |
| IP Address | The IP address associated with this record. |
| TTL | The time to live reported by the name server. |
| Domain | The domain name associated with this record. |

## show hosts

This command displays the static host name-to-address mapping table.

### COMMAND MODE

Privileged Exec

### EXAMPLE

Note that a host name will be displayed as an alias if it is mapped to the same address(es) as a previously configured entry.

```
Console#show hosts
No.  Flag Type    IP Address           TTL   Domain
---- ---- ------- --------------------  ----- --------------------------------
   0    2 Address 192.168.1.55               rd5
   1    2 Address 2001:DB8:1::12             rd6
   3    4 Address 209.131.36.158             65 www-real.wa1.b.yahoo.com
   4    4 CNAME   POINTER TO:3               65 www.yahoo.com
   5    4 CNAME   POINTER TO:3               65 www.wa1.b.yahoo.com
Console#
```

**Table 3: show hosts** - display description

| **Field** | **Description** |
|---|---|
| No. | The entry number for each resource record. |
| Flag | The field displays “2” for a static entry, or “4” for a dynamic entry stored in the cache. |
| Type | This field includes “Address” which specifies the primary name for the owner, and “CNAME” which specifies multiple domain names (or aliases) which are mapped to the same IP address as an existing entry. |
| IP Address | The IP address associated with this record. |
| TTL | The time to live reported by the name server. This field is always blank for static entries. |
| Domain | The domain name associated with this record. |

# 45 DHCP COMMANDS

These commands are used to configure Dynamic Host Configuration Protocol (DHCP) client, relay, and server functions. Any VLAN interface can be configured to automatically obtain an IPv4 address through DHCP. This switch can be configured to relay DHCP client configuration requests to a DHCP server on another network, or it can be configured to provide DHCP service directly to any client.

**Table 1: DHCP Commands**

| Command Group | Function |
|---|---|
| DHCP Client | Allows interfaces to dynamically acquire IPv4 address information |
| DHCP Relay | Relays DHCP requests from local hosts to a remote DHCP server |
| DHCP Server | Configures DHCP service using address pools or static bindings |

## DHCP CLIENT

Use the commands in this section to allow the switch's VLAN interfaces to dynamically acquire IP address information.

**Table 2: DHCP Client Commands**

| Command | Function | Mode |
|---|---|---|
| *DHCP for IPv4* | | |
| ip dhcp client class-id | Specifies the DHCP vendor class identifier for an interface | IC |
| ip dhcp restart client | Submits a BOOTP or DHCP client request | PE |
| *DHCP for IPv6* | | |
| ipv6 dhcp client rapid-commit vlan | Specifies the Rapid Commit option for DHCPv6 message exchange | GC |

### ip dhcp client class-id

This command specifies the DCHP vendor class identifier for the current interface. Use the **no** form to remove this identifier.

**SYNTAX**

**ip dhcp client class-id** {**text** *text* | **hex** *hex*}

**no ip dhcp client class-id**

*text* - A text string. (Range: 1-32 characters)

*hex* - A hexadecimal value.

### DEFAULT SETTING
EL 326

### COMMAND MODE
Interface Configuration (VLAN)

### COMMAND USAGE
- The class identifier is used identify the vendor class and configuration of the switch to the DHCP server, which then uses this information to decide on how to service the client or the type of information to return.
- The general framework for this DHCP option is set out in RFC 2132 (Option 60). This information is used to convey configuration settings or other identification information about a client, but the specific string to use should be supplied by your service provider or network administrator.

### EXAMPLE

```
Console(config)#interface vlan 2
Console(config-if)#ip dhcp client class-id hex 000099669966
Console(config-if)#
```

### RELATED COMMANDS
ip dhcp restart client (1040)

## ip dhcp restart client

This command submits a BOOTP or DHCP client request.

### DEFAULT SETTING
None

### COMMAND MODE
Privileged Exec

### COMMAND USAGE
- This command issues a BOOTP or DHCP client request for any IP interface that has been set to BOOTP or DHCP mode through the ip address command.
- DHCP requires the server to reassign the client's last address if available.
- If the BOOTP or DHCP server has been moved to a different domain, the network portion of the address provided to the client will be based on this new domain.

#### EXAMPLE

In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart client
Console#show ip interface
Vlan 1 is Administrative Up - Link Up
  Address is 12-34-12-34-12-34 (bia 12-34-12-34-12-34)
  Index: 1001, MTU: 1500, Bandwidth: 1g
  Address Mode is DHCP
  IP Address: 192.168.0.9 Mask: 255.255.255.0
  Proxy ARP is disabled
Console#
```

#### RELATED COMMANDS

ip address (1068)

### ipv6 dhcp client rapid-commit vlan

This command specifies the Rapid Commit option for DHCPv6 message exchange for all DHCPv6 client requests submitted from the specified interface. Use the **no** form to disable this option.

#### SYNTAX

[**no**] **ipv6 dhcp client rapid-commit vlan** *vlan-id*

*vlan-id* - VLAN ID, specified as a single number, a range of consecutive numbers separated by a hyphen, or multiple numbers separated by commas. (Range: 1-4093, no leading zeroes)

#### DEFAULT SETTING

Disabled

#### COMMAND MODE

Global Configuration

#### COMMAND USAGE

- DHCPv6 clients can obtain configuration parameters from a server through a normal four-message exchange (solicit, advertise, request, reply), or through a rapid two-message exchange (solicit, reply). The rapid-commit option must be enabled on both client and server for the two-message exchange to be used.
- This command allows two-message exchange method for prefix delegation. When enabled, DCHPv6 client requests submitted from the specified interface will include the rapid commit option in all solicit messages.

#### EXAMPLE

```
Console(config)#ipv6 dhcp client rapid-commit vlan 2
Console(config)#
```

# DHCP RELAY

This section describes commands used to configure DHCP relay functions for host devices attached to the switch.

**Table 3: DHCP Relay Commands**

| Command | Function | Mode |
|---|---|---|
| ip dhcp relay server | Specifies DHCP server addresses for relay | IC |
| ip dhcp restart relay | Enables DHCP relay agent | PE |

## ip dhcp relay server

This command specifies the addresses of DHCP servers to be used by the switch's DHCP relay agent. Use the **no** form to clear all addresses.

### SYNTAX

**ip dhcp relay server** *address1* [*address2* [*address3* ...]]

**no ip dhcp relay server**

*address* - IP address of DHCP server. (Range: 1-3 addresses)

### DEFAULT SETTING

None

### COMMAND MODE

Interface Configuration (VLAN)

### USAGE GUIDELINES

- You must specify the IP address for at least one DHCP server. Otherwise, the switch's DHCP relay agent will not forward client requests to a DHCP server.
- To start DHCP relay service, enter the ip dhcp restart relay command.

### EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip dhcp relay server 10.1.0.99
Console(config-if)#
```

### RELATED COMMANDS

ip dhcp restart relay (1042)

## ip dhcp restart relay

This command enables DHCP relay for the specified VLAN. Use the **no** form to disable it.

### DEFAULT SETTING

Disabled

#### COMMAND MODE

Privileged Exec

#### COMMAND USAGE

This command is used to configure DHCP relay functions for host devices attached to the switch. If DHCP relay service is enabled, and this switch sees a DHCP request broadcast, it inserts its own IP address into the request so the DHCP server will know the subnet where the client is located. Then, the switch forwards the packet to the DHCP server on another network. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client's subnet, and sends a DHCP response back to the DHCP relay agent (i.e., this switch). This switch then broadcasts the DHCP response received from the server to the client.

#### EXAMPLE

In the following example, the device is reassigned the same address.

```
Console(config)#ip dhcp restart relay
Console(config)#end
Console#show ip interface

Vlan 1 is up, addressing mode is Dhcp
  Interface address is 10.1.0.254, mask is 255.255.255.0, Primary
  MTU is 1500 bytes
  Proxy ARP is disabled
  Split horizon is enabled
Console#
```

#### RELATED COMMANDS

ip dhcp relay server (1042)

## DHCP SERVER

This section describes commands used to configure client address pools for the DHCP service.

**Table 4: DHCP Server Commands**

| Command | Function | Mode |
|---|---|---|
| ip dhcp excluded-address | Specifies IP addresses that a DHCP server should not assign to DHCP clients | GC |
| ip dhcp pool | Configures a DHCP address pool on a DHCP Server | GC |
| service dhcp | Enables the DHCP server feature on this switch | GC |
| bootfile | Specifies a default boot image for a DHCP client | DC |
| client-identifier[1] | Specifies a client identifier for a DHCP client | DC |
| default-router | Specifies the default router list for a DHCP client | DC |
| dns-server | Specifies the Domain Name Server (DNS) servers available to a DHCP client | DC |
| domain-name | Specifies the domain name for a DHCP client | DC |

**Table 4: DHCP Server Commands**

| Command | Function | Mode |
|---|---|---|
| hardware-address[1] | Specifies the hardware address of a DHCP client | DC |
| host[1] | Specifies the IP address and network mask to manually bind to a DHCP client | DC |
| lease | Sets the duration an IP address is assigned to a DHCP client | DC |
| netbios-name-server | Configures NetBIOS Windows Internet Naming Service (WINS) name servers available to Microsoft DHCP clients | DC |
| netbios-node-type | Configures NetBIOS node type for Microsoft DHCP clients | DC |
| network | Configures the subnet number and mask for a DHCP address pool | DC |
| next-server | Configures the next server in the boot process of a DHCP client | DC |
| clear ip dhcp binding | Deletes an automatic address binding from the DHCP server database | PE |
| show ip dhcp binding | Displays address bindings on the DHCP server | PE, NE |
| show ip dhcp | Displays DHCP address pools | PE |

1. These commands are used for manually binding an address to a client.

## ip dhcp excluded-address

This command specifies IP addresses that the DHCP server should not assign to DHCP clients. Use the **no** form to remove the excluded IP addresses.

### SYNTAX

[**no**] **ip dhcp excluded-address** *low-address* [*high-address*]

*low-address* - An excluded IP address, or the first IP address in an excluded address range.

*high-address* - The last IP address in an excluded address range.

### DEFAULT SETTING

All IP pool addresses may be assigned.

### COMMAND MODE

Global Configuration

### EXAMPLE

```
Console(config)#ip dhcp excluded-address 10.1.0.19
Console(config)#
```

## ip dhcp pool

This command configures a DHCP address pool and enter DHCP Pool Configuration mode. Use the **no** form to remove the address pool.

### SYNTAX

[**no**] **ip dhcp pool** *name*

*name* - A string or integer. (Range: 1-8 characters)

#### DEFAULT SETTING
DHCP address pools are not configured.

#### COMMAND MODE
Global Configuration

#### USAGE GUIDELINES
- After executing this command, the switch changes to DHCP Pool Configuration mode, identified by the (config-dhcp)# prompt.
- From this mode, first configure address pools for the network interfaces (using the network command). You can also manually bind an address to a specific client (with the host command) if required. You can configure up to 8 network address pools, and up to 32 manually bound host address pools (i.e., listing one host address per pool). However, note that any address specified in a host command must fall within the range of a configured network address pool.

#### EXAMPLE
```
Console(config)#ip dhcp pool R&D
Console(config-dhcp)#
```

#### RELATED COMMANDS
network (1052)
host (1049)

## service dhcp

This command enables the DHCP server on this switch. Use the **no** form to disable the DHCP server.

#### SYNTAX

[**no**] **service dhcp**

#### DEFAULT SETTING
Enabled

#### COMMAND MODE
Global Configuration

#### COMMAND USAGE
If the DHCP server is running, you must restart it to implement any configuration changes.

#### EXAMPLE
```
Console(config)#service dhcp
Console(config)#
```

## bootfile

This command specifies the name of the default boot image for a DHCP client. This file should placed on the Trivial File Transfer Protocol (TFTP) server specified with the next-server command. Use the **no** form to delete the boot image name.

### Syntax

**bootfile** *filename*

**no bootfile**

*filename* - Name of the file that is used as a default boot image.

### Default Setting

None

### Command Mode

DHCP Pool Configuration

### Example

```
Console(config-dhcp)#bootfile wme.bat
Console(config-dhcp)#
```

### Related Commands

next-server (1053)

## client-identifier

This command specifies the client identifier of a DHCP client. Use the **no** form to remove the client identifier.

### Syntax

**client-identifier** {**text** *text* | **hex** *hex*}

**no client-identifier**

*text* - A text string. (Range: 1-15 characters)

*hex* - The hexadecimal value.

### Default Setting

None

### Command Mode

DHCP Pool Configuration

### Command Usage

- This command identifies a DHCP client to bind to an address specified in the host command. If both a client identifier and hardware address are configured for a host address, the client identifier takes precedence over the hardware address in the search procedure.

- BOOTP clients cannot transmit a client identifier. To bind an address to a BOOTP client, you must associate a hardware address with the host entry.

#### EXAMPLE

```
Console(config-dhcp)#client-identifier text steve
Console(config-dhcp)#
```

#### RELATED COMMANDS

host (1049)

### default-router

This command specifies default routers for a DHCP pool. Use the **no** form to remove the default routers.

#### SYNTAX

**default-router** *address1* [*address2*]

**no default-router**

*address1* - Specifies the IP address of the primary router.

*address2* - Specifies the IP address of an alternate router.

#### DEFAULT SETTING

None

#### COMMAND MODE

DHCP Pool Configuration

#### USAGE GUIDELINES

The IP address of the router should be on the same subnet as the client. You can specify up to two routers. Routers are listed in order of preference (starting with *address1* as the most preferred router).

#### EXAMPLE

```
Console(config-dhcp)#default-router 10.1.0.54 10.1.0.64
Console(config-dhcp)#
```

### dns-server

This command specifies the Domain Name System (DNS) IP servers available to a DHCP client. Use the **no** form to remove the DNS server list.

#### SYNTAX

**dns-server** *address1* [*address2*]

**no dns-server**

*address1* - Specifies the IP address of the primary DNS server.

*address2* - Specifies the IP address of the alternate DNS server.

#### DEFAULT SETTING

None

### COMMAND MODE
DHCP Pool Configuration

### USAGE GUIDELINES
- If DNS IP servers are not configured for a DHCP client, the client cannot correlate host names to IP addresses.
- Servers are listed in order of preference (starting with *address1* as the most preferred server).

### EXAMPLE
```
Console(config-dhcp)#dns-server 10.1.1.253 192.168.3.19
Console(config-dhcp)#
```

## domain-name

This command specifies the domain name for a DHCP client. Use the **no** form to remove the domain name.

### SYNTAX
**domain-name** *domain*

**no domain-name**

*domain* - Specifies the domain name of the client.
(Range: 1-32 characters)

### DEFAULT SETTING
None

### COMMAND MODE
DHCP Pool Configuration

### EXAMPLE
```
Console(config-dhcp)#domain-name sample.com
Console(config-dhcp)#
```

## hardware-address

This command specifies the hardware address of a DHCP client. This command is valid for manual bindings only. Use the **no** form to remove the hardware address.

### SYNTAX

**hardware-address** *hardware-address type*

**no hardware-address**

*hardware-address* - Specifies the MAC address of the client device.

*type* - Indicates the following protocol used on the client device:

- ethernet
- ieee802
- fddi

### DEFAULT SETTING

If no type is specified, the default protocol is Ethernet.

### COMMAND MODE

DHCP Pool Configuration

### COMMAND USAGE

This command identifies a DHCP or BOOTP client to bind to an address specified in the host command. BOOTP clients cannot transmit a client identifier. To bind an address to a BOOTP client, you must associate a hardware address with the host entry.

### EXAMPLE

```
Console(config-dhcp)#hardware-address 00-e0-29-94-34-28 ethernet
Console(config-dhcp)#
```

### RELATED COMMANDS

host (1049)

## host

Use this command to specify the IP address and network mask to manually bind to a DHCP client. Use the **no** form to remove the IP address for the client.

### SYNTAX

**host** *address* [*mask*]

**no host**

*address* - Specifies the IP address of a client.

*mask* - Specifies the network mask of the client.

### DEFAULT SETTING

None

### COMMAND MODE

DHCP Pool Configuration

### USAGE GUIDELINES

- Host addresses must fall within the range specified for an existing network pool.
- When a client request is received, the switch first checks for a network address pool matching the gateway where the request originated (i.e., if the request was forwarded by a relay server). If there is no gateway in the client request (i.e., the request was not forwarded by a relay server), the switch searches for a network pool matching the interface through which the client request was received. It then searches for a manually configured host address that falls within the matching network pool.
- When searching for a manual binding, the switch compares the client identifier for DHCP clients, and then compares the hardware address for DHCP or BOOTP clients.
- If no manual binding has been specified for a host entry with the client-identifier or hardware-address commands, then the switch will assign an address from the matching network pool.
- If the mask is unspecified, DHCP examines its address pools. If no mask is found in the pool database, the Class A, B, or C natural mask is used (see page 1052). This command is valid for manual bindings only.
- The **no host** command only clears the address from the DHCP server database. It does not cancel the IP address currently in use by the host.

### EXAMPLE

```
Console(config-dhcp)#host 10.1.0.21 255.255.255.0
Console(config-dhcp)#
```

### RELATED COMMANDS

client-identifier (1046)
hardware-address (1049)

## lease

This command configures the duration that an IP address is assigned to a DHCP client. Use the **no** form to restore the default value.

### SYNTAX

**lease** {*days* [*hours*][*minutes*] | **infinite**}

**no lease**

*days* - Specifies the duration of the lease in numbers of days. (Range: 0-364)

*hours* - Specifies the number of hours in the lease. A *days* value must be supplied before you can configure *hours*. (Range: 0-23)

*minutes* - Specifies the number of minutes in the lease. A *days* and *hours* value must be supplied before you can configure *minutes*. (Range: 0-59)

**infinite** - Specifies that the lease time is unlimited. This option is normally used for addresses manually bound to a BOOTP client via the **host** command.

#### DEFAULT SETTING
One day

#### COMMAND MODES
DHCP Pool Configuration

#### EXAMPLE
The following example leases an address to clients using this pool for 7 days.

```
Console(config-dhcp)#lease 7
Console(config-dhcp)#
```

### netbios-name-server

This command configures NetBIOS Windows Internet Naming Service (WINS) name servers that are available to Microsoft DHCP clients. Use the **no** form to remove the NetBIOS name server list.

#### SYNTAX

**netbios-name-server** *address1* [*address2*]

**no netbios-name-server**

*address1* - Specifies IP address of primary NetBIOS WINS name server.

*address2* - Specifies IP address of alternate NetBIOS WINS name server.

#### DEFAULT SETTING
None

#### COMMAND MODE
DHCP Pool Configuration

#### USAGE GUIDELINES
Servers are listed in order of preference (starting with *address1* as the most preferred server).

#### EXAMPLE

```
Console(config-dhcp)#netbios-name-server 10.1.0.33 10.1.0.34
Console(config-dhcp)#
```

#### RELATED COMMANDS
netbios-node-type (1052)

## netbios-node-type

This command configures the NetBIOS node type for Microsoft DHCP clients. Use the **no** form to remove the NetBIOS node type.

### Syntax

**netbios-node-type** *type*

**no netbios-node-type**

*type* - Specifies the NetBIOS node type:

**broadcast**

**hybrid** (recommended)

**mixed**

**peer-to-peer**

### Default Setting

None

### Command Mode

DHCP Pool Configuration

### Example

```
Console(config-dhcp)#netbios-node-type hybrid
Console(config-dhcp)#
```

### Related Commands

netbios-name-server (1051)

## network

This command configures the subnet number and mask for a DHCP address pool. Use the **no** form to remove the subnet number and mask.

### Syntax

**network** *network-number* [*mask*]

**no network**

*network-number* - The IP address of the DHCP address pool.

*mask* - The bit combination that identifies the network (or subnet) and the host portion of the DHCP address pool.

### Command Mode

DHCP Pool Configuration

### Usage Guidelines

- When a client request is received, the switch first checks for a network address pool matching the gateway where the request originated (i.e., if the request was forwarded by a relay server). If there is no gateway in the client request (i.e., the request was not forwarded by a relay server), the switch searches for a network pool matching the interface through which the client request was received. It then searches for a manually configured host address that falls within the matching network pool. If no manually configured host address is found, it assigns an address from the matching network address pool. However, if no matching address pool is found the request is ignored.

- This command is valid for DHCP network address pools only. If the mask is not specified, the class A, B, or C natural mask is used. Subnet addresses are interpreted as class A, B or C, based on the first field in the specified address. In other words, if a subnet address nnn.xxx.xxx.xxx is entered, the first field (nnn) determines the class:

  0 - 127 is class A, only uses the first field in the network address.
  128 - 191 is class B, uses the first two fields in the network address.
  192 - 223 is class C, uses the first three fields in the network address.

- The DHCP server assumes that all host addresses are available. You can exclude subsets of the address space by using the ip dhcp excluded-address command.

### EXAMPLE

```
Console(config-dhcp)#network 10.1.0.0 255.255.255.0
Console(config-dhcp)#
```

## next-server

This command configures the next server in the boot process of a DHCP client. Use the **no** form to remove the boot server list.

### SYNTAX

[**no**] **next-server** *address*

*address* - Specifies the IP address of the next server in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server.

### DEFAULT SETTING

None

### COMMAND MODE

DHCP Pool Configuration

### EXAMPLE

```
Console(config-dhcp)#next-server 10.1.0.21
Console(config-dhcp)#
```

### RELATED COMMANDS

bootfile (1046)

## clear ip dhcp binding

This command deletes an automatic address binding from the DHCP server database.

#### Syntax

**clear ip dhcp binding** {*address* | *}

*address* - The address of the binding to clear.

* - Clears all automatic bindings.

#### Default Setting

None

#### Command Mode

Privileged Exec

#### Usage Guidelines

- An *address* specifies the client's IP address. If an asterisk (*) is used as the address parameter, the DHCP server clears all automatic bindings.
- Use the no host command to delete a manual binding.
- This command is normally used after modifying the address pool, or after moving DHCP service to another device.

#### Example.

```
Console#clear ip dhcp binding *
Console#
```

#### Related Commands

show ip dhcp binding (1054)

### show ip dhcp binding

This command displays address bindings on the DHCP server.

#### Syntax

**show ip dhcp binding** [*address*]

*address* - Specifies the IP address of the DHCP client for which bindings will be displayed.

#### Default Setting

None

#### Command Mode

Normal Exec, Privileged Exec

#### Example

```
Console#show ip dhcp binding

     IP            MAC          Lease Time        Start
                             (dd/hh/mm/ss)
--------------- ---------------- ------------------ -----------
```

```
    192.1.3.21 00-00-e8-98-73-21          86400 Dec 25 08:01:57 2002
Console#
```

**show ip dhcp** This command displays DHCP address pools configured on the switch.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show ip dhcp

  Name   Type   IP Address        Mask               Active Pool
-------- ---- --------------- --------------- --------------------------------
tps      Net  192.168.1.0     255.255.255.0   192.168.1.1     - 192.168.1.254

Total entry : 1
Console#
```

# 46 VRRP COMMANDS

Virtual Router Redundancy Protocol (VRRP) use a virtual IP address to support a primary router and multiple backup routers. The backup routers can be configured to take over the workload if the master router fails, or can also be configured to share the traffic load. The primary goal of router redundancy is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

To configure VRRP, select an interface on each router in the group that will participate in the protocol as the master router or a backup router. To select a specific device as the master router, set the address of this interface as the virtual router address for the group. Now set the same virtual address and a priority on the backup routers, and configure an authentication string. You can also enable the preempt feature which allows a router to take over as the master router when it comes on line if it has a higher priority than the currently active master router.

**Table 1: VRRP Commands**

| Command | Function | Mode |
|---|---|---|
| vrrp accept mode | Configures the router to allow the master to respond to the virtual IP address, even if it is not the IP address owner. | IC |
| vrrp authentication | Configures a key used to authenticate VRRP packets received from other routers | IC |
| vrrp ip | Enables VRRP and sets the IP address of the virtual router | IC |
| vrrp preempt | Configures the router to take over as master virtual router for a VRRP group if it has a higher priority than the current master virtual router | IC |
| vrrp priority | Sets the priority of this router in the VRRP group | IC |
| vrrp timers advertise | Sets the interval between successive advertisements by the master virtual router | IC |
| clear vrrp interface counters | Clears VRRP interface statistics | PE |
| clear vrrp router counters | Clears VRRP router statistics | PE |
| show vrrp | Displays VRRP status information | PE |
| show vrrp interface | Displays VRRP status information for the specified interface | PE |
| show vrrp interface counters | Displays VRRP statistics for the specified interface | PE |
| show vrrp router counters | Displays VRRP statistics | PE |

## vrrp accept mode

This command configures the router to allow the master to respond to the virtual IP address, even if it is not the IP address owner.

### SYNTAX

**vrrp** *group* **accept-mode**

**no vrrp** *group* **accept-mode**

*group* - Identifies the virtual router group. (Range: 1-255)

### DEFAULT SETTING

Accept-Mode: Disabled.

### COMMAND MODE

Interface (VLAN)

### COMMAND USAGE

- If accept mode is enabled, it disables the installation of routes for the Virtual Router Redundancy Protocol (VRRP) virtual address. This allows the master to respond to the virtual IP address, even if it is not the IP address owner.

### EXAMPLE

```
Console(config-if)#vrrp 1 accept-mode
Console(config-if)#
```

## vrrp authentication

This command specifies the key used to authenticate VRRP packets received from other routers. Use the **no** form to prevent authentication.

### SYNTAX

**vrrp** *group* **authentication** *key*

**no vrrp** *group* **authentication**

*group* - Identifies the virtual router group. (Range: 1-255)

*key* - Authentication string. (Range: 1-8 alphanumeric characters)

### DEFAULT SETTING

No key is defined.

### COMMAND MODE

Interface (VLAN)

### COMMAND USAGE

- All routers in the same VRRP group must be configured with the same authentication key.

- When a VRRP packet is received from another router in the group, its authentication key is compared to the string configured on this router. If the keys match, the message is accepted. Otherwise, the packet is discarded.

- Plain text authentication does not provide any real security. It is supported only to prevent a misconfigured router from participating in VRRP.

#### EXAMPLE

```
Console(config-if)#vrrp 1 authentication bluebird
Console(config-if)#
```

### vrrp ip

This command enables the Virtual Router Redundancy Protocol (VRRP) on an interface and specifies the IP address of the virtual router. Use the **no** form to disable VRRP on an interface and remove the IP address from the virtual router.

#### SYNTAX

[**no**] **vrrp** *group* **ip** *ip-address*

*group* - Identifies the virtual router group. (Range: 1-255)

*ip-address* - The IP address of the virtual router. This is the IP address that end-hosts set as their default gateway.

#### DEFAULT SETTING

No virtual router groups are configured.

#### COMMAND MODE

Interface (VLAN)

#### COMMAND USAGE

- The interfaces of all routers participating in a virtual router group must be within the same IP subnet.
- If the IP address assigned to the virtual router with this command is already configured as the primary address on this interface, this router is considered the Owner, and will assume the role of the Master virtual router in the group.
- This interface is used for two purposes - to send/receive advertisement messages and to forward on behalf of the virtual router when operating as the Master VRRP router.
- VRRP is enabled as soon as this command is entered. If you need to customize any of the other parameters for VRRP such as authentication, priority, or advertisement interval, then first configure these parameters before enabling VRRP.

#### EXAMPLE

This example creates VRRP group 1 using the primary interface for VLAN 1 as the VRRP group Owner.

```
Console(config)#interface vlan 1
Console(config-if)#vrrp 1 ip 192.168.1.6
Console(config-if)#
```

## vrrp preempt

This command configures the router to take over as the master virtual router for a VRRP group if it has a higher priority than the current acting master router. Use the **no** form to disable preemption.

### SYNTAX

**vrrp** *group* **preempt** [**delay** *seconds*]

**no vrrp** *group* **preempt**

*group* - Identifies the VRRP group. (Range: 1-255)

*seconds* - The time to wait before issuing a claim to become the master. (Range: 0-120 seconds)

### DEFAULT SETTING

Preempt: Enabled
Delay: 0 seconds

### COMMAND MODE

Interface (VLAN)

### COMMAND USAGE

- If preempt is enabled, and this backup router has a priority higher than the current acting master, it will take over as the new master. However, note that if the original master (i.e., the owner of the VRRP IP address) comes back on line, it will always resume control as the master.
- The delay can give additional time to receive an advertisement message from the current master before taking control. If the router attempting to become the master has just come on line, this delay also gives it time to gather information for its routing table before actually preempting the currently active router.

### EXAMPLE

```
Console(config-if)#vrrp 1 preempt delay 10
Console(config-if)#
```

### RELATED COMMANDS

vrrp priority (1060)

## vrrp priority

This command sets the priority of this router in a VRRP group. Use the **no** form to restore the default setting.

### SYNTAX

**vrrp** *group* **priority** *level*

**no vrrp** *group* **priority**

*group* - Identifies the VRRP group. (Range: 1-255)

*level* - Priority of this router in the VRRP group. (Range: 1-254)

### DEFAULT SETTING
Master: 255
Backup: 100

### COMMAND MODE
Interface (VLAN)

### COMMAND USAGE
- A router that has a physical interface with the same IP address as that used for the virtual router (that is, the owner of the VRRP IP address) will become the master virtual router. The backup router with the highest priority will become the master router if the current master fails. When the original master router recovers, it will take over as the active master router again.
- If two or more routers are configured with the same VRRP priority, the router with the highest IP address is elected as the new master router if the current master fails.
- If the backup preempt function is enabled with the vrrp preempt command, and a backup router with a priority higher than the current acting master comes on line, this backup router will take over as the new acting master. However, note that if the original master (i.e., the owner of the VRRP IP address) comes back on line, it will always resume control as the master.
- If the virtual IP address for the VRRP group is the same as that of the configured device, the priority will automatically be set to 255 prior to using this command.

### EXAMPLE
```
Console(config-if)#vrrp 1 priority 1
Console(config-if)#
```

### RELATED COMMANDS
vrrp preempt (1060)

## vrrp timers advertise

This command sets the interval at which the master virtual router sends advertisements communicating its state as the master. Use the **no** form to restore the default interval.

### SYNTAX

**vrrp** *group* **timers advertise** *interval*

**no vrrp** *group* **timers advertise**

*group* - Identifies the VRRP group. (Range: 1-255)

*interval* - Advertisement interval for the master virtual router. (Range: 1-255 seconds)

### DEFAULT SETTING
1 second

**COMMAND MODE**
Interface (VLAN)

**COMMAND USAGE**

- VRRP advertisements from the current master virtual router include information about its priority and current state as the master.
- VRRP advertisements are sent to the multicast address 224.0.0.18. Using a multicast address reduces the amount of traffic that has to processed by network devices that are not part of the designated VRRP group.
- If the master router stops sending advertisements, backup routers will bid to become the master router based on priority. The dead interval before attempting to take over as the master is three times the hello interval plus half a second

**EXAMPLE**

```
Console(config-if)#vrrp 1 timers advertise 5
Console(config-if)#
```

## clear vrrp interface counters

This command clears VRRP system statistics for the specified group and interface.

**clear vrrp** *group* **interface** *interface* **counters**

*group* - Identifies a VRRP group. (Range: 1-255)

*interface* - Identifier of configured VLAN interface. (Range: 1-4093)

**DEFAULTS**
None

**COMMAND MODE**
Privileged Exec

**EXAMPLE**

```
Console#clear vrrp 1 interface 1 counters
Console#
```

## clear vrrp router counters

This command clears VRRP system statistics.

**COMMAND MODE**
Privileged Exec

**EXAMPLE**

```
Console#clear vrrp router counters
Console#
```

## show vrrp

This command displays status information for VRRP.

### SYNTAX

**show vrrp** [**brief** | *group*]

**brief** - Displays summary information for all VRRP groups on this router.

*group* - Identifies a VRRP group. (Range: 1-255)

### DEFAULTS

None

### COMMAND MODE

Privileged Exec

### COMMAND USAGE

- Use this command without any keywords to display the full listing of status information for all VRRP groups configured on this router.
- Use this command with the **brief** keyword to display a summary of status information for all VRRP groups configured on this router.
- Specify a group number to display status information for a specific group

### EXAMPLE

This example displays the full listing of status information for all groups.

```
Console#show vrrp
 Vlan 1 - Group 1,
 State                          Master
 Virtual IP Address                  192.168.1.6
 Virtual MAC Address                   00-00-5E-00-01-01
 Advertisement Interval                5 sec
 Preemption                         Enabled
 Min Delay                         10 sec
 Priority                       255
 Authentication                     SimpleText
 Authentication Key                   bluebird
 Master Router                      192.168.1.6
 Master Priority                   255
 Master Advertisement Interval    5 sec
 Master Down Interval               15
Console#
```

**Table 2: show vrrp** - display description

| Field | Description |
|---|---|
| State | VRRP role of this interface (master or backup) |
| Virtual IP address | Virtual address that identifies this VRRP group |
| Virtual MAC address | Virtual MAC address derived from the owner of the virtual IP address |
| Advertisement interval | Interval at which the master virtual router advertises its role as the master |

**Table 2: show vrrp** - display description (Continued)

| Field | Description |
|---|---|
| Preemption | Shows whether or not a higher priority router can preempt the current acting master |
| Min delay | Delay before a router with a higher priority can preempt the current acting master |
| Priority | Priority of this router |
| Authentication | Authentication mode used to verify VRRP packets |
| Authentication key | Key used to authenticate VRRP packets received from other routers |
| Master Router | IP address of the router currently acting as the VRRP group master |
| Master priority | The priority of the router currently acting as the VRRP group master |
| Master Advertisement interval | The advertisement interval configured on the VRRP master. |
| Master down interval | The down interval configured on the VRRP master (This interval is used by all the routers in the group regardless of their local settings) |

This example displays the brief listing of status information for all groups.

```
Console#show vrrp brief
Interface   Grp   State   Virtual Addr    Interval  Preempt  Priority
---------- ----- -------- ---------------- ----------- --------- --------
VLAN 1       1  Master      192.168.0.3         1  E          255
Console#
```

**Table 3: show vrrp brief** - display description

| Field | Description |
|---|---|
| Interface | VLAN interface |
| Grp | VRRP group |
| State | VRRP role of this interface (master or backup) |
| Virtual Addr | Virtual address that identifies this VRRP group |
| Interval | Interval at which the master virtual router advertises its role as the master |
| Preempt | Shows whether or not a higher priority router can preempt the current acting master |
| Priority | Priority of this router |

## show vrrp interface

This command displays status information for the specified VRRP interface.

### SYNTAX

**show vrrp interface vlan** *vlan-id* [**brief**]

*vlan-id* - Identifier of configured VLAN interface. (Range: 1-4093)

**brief** - Displays summary information for all VRRP groups on this router.

**DEFAULTS**
None

**COMMAND MODE**
Privileged Exec

**EXAMPLE**
This example displays the full listing of status information for VLAN 1.

```
Console#show vrrp interface vlan 1
 Vlan 1 - Group 1,
 State                          Master
 Virtual IP Address             192.168.1.6
 Virtual MAC Address            00-00-5E-00-01-01
 Advertisement Interval         5 sec
 Preemption                     Enabled
 Min Delay                      10 sec
 Priority                       1
 Authentication                 SimpleText
 Authentication Key             bluebird
 Master Router                  192.168.1.6
 Master Priority                1
 Master Advertisement Interval  5 sec
 Master Down Interval           15
Console#
```

* Refer to the show vrrp command for a description of the display items.

## show vrrp interface counters

This command displays counters for VRRP protocol events and errors that have occurred for the specified group and interface.

**show vrrp** *group* **interface vlan** *interface* **counters**

*group* - Identifies a VRRP group. (Range: 1-255)

*interface* - Identifier of configured VLAN interface. (Range: 1-4093)

**DEFAULTS**
None

**COMMAND MODE**
Privileged Exec

**EXAMPLE**

```
Console#show vrrp 1 interface vlan 1 counters
 Total Number of Times Transitioned to MASTER                      : 6
 Total Number of Received Advertisements Packets                   : 0
 Total Number of Received Error Advertisement Interval Packets     : 0
 Total Number of Received Authentication Failures Packets          : 0
 Total Number of Received Error IP TTL VRRP Packets                : 0
 Total Number of Received Priority 0 VRRP Packets                  : 0
 Total Number of Sent Priority 0 VRRP Packets                      : 5
 Total Number of Received Invalid Type VRRP Packets                : 0
 Total Number of Received Error Address List VRRP Packets          : 0
 Total Number of Received Invalid Authentication Type VRRP Packets : 0
```

```
 Total Number of Received Mismatch Authentication Type VRRP Packets : 0
 Total Number of Received Error Packet Length VRRP Packets         : 0
Console#
```

* Refer to ?$paratext>? on page 462 for a description of the display items.

## show vrrp router counters

This command displays counters for errors found in VRRP protocol packets.

### Command Mode

Privileged Exec

### Example

Note that unknown errors indicate VRRP packets received with an unknown or unsupported version number.

```
Console#show vrrp router counters
 Total Number of VRRP Packets with Invalid Checksum : 0
 Total Number of VRRP Packets with Unknown Error    : 0
 Total Number of VRRP Packets with Invalid VRID     : 0
Console#
```

# 47 IP INTERFACE COMMANDS

An IP Version 4 and Version 6 address may be used for management access to the switch over the network. Both IPv4 or IPv6 addresses can be used simultaneously to access the switch. You can manually configure a specific IPv4 or IPv6 address or direct the switch to obtain an IPv4 address from a BOOTP or DHCP server when it is powered on. An IPv6 address can either be manually configured or dynamically generated.

An IPv4 address for this switch is obtained via DHCP by default for VLAN 1. You may also need to a establish an IPv4 or IPv6 default gateway between this device and management stations that exist on another network segment.

**Table 1: IP Interface Commands**

| Command Group | Function |
|---|---|
| IPv4 Interface | Configures an IPv4 address for the switch |
| IPv6 Interface | Configures an IPv6 address for the switch |
| IPv6 to IPv4 Tunnels | Configures IPv6 over IPv4 tunnels |

## IPV4 INTERFACE

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 or to connect the switch to existing IP subnets. You may also need to a establish a default gateway between this device and management stations or other devices that exist on another network segment (if routing is not enabled).

This section includes commands for configuring IP interfaces, the Address Resolution Protocol (ARP) and Proxy ARP.

**Table 2: IPv4 Interface Commands**

| Command Group | Function |
|---|---|
| Basic IPv4 Configuration | Configures the IP address for interfaces and the gateway router |
| ARP Configuration | Configures static, dynamic and proxy ARP service |
| UDP Helper Configuration | Forwards UDP broadcast packets to a specified server |

## BASIC IPV4 CONFIGURATION

This section describes commands used to configure IP addresses for VLAN interfaces on the switch.

**Table 3: Basic IP Configuration Commands**

| Command | Function | Mode |
|---|---|---|
| ip address | Sets the IP address for the current interface | IC |
| ip default-gateway | Defines the default gateway through which this router can reach other subnetworks | GC |
| show ip interface | Displays the IP settings for this device | PE |
| show ip route | Displays specified entries in the routing table | PE |
| traceroute | Shows the route packets take to the specified host | PE |
| ping | Sends ICMP echo request packets to another node on the network | NE, PE |

## ip address

This command sets the IPv4 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 any network interfaces are configured on the router, 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.

- An IP address must be assigned to this device to gain management access over the network or to connect the router to existing IP subnets. A specific IP address can be manually configured, or the router can be directed to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Anything other than this format is not be accepted by the configuration program.

- An interface can have only one primary IP address, but can have many secondary IP addresses. In other words, secondary addresses need to be specified if more than one IP subnet can be accessed through this interface. Note that a secondary address cannot be configured prior to setting the primary IP address, and the primary address cannot be removed if a secondary address is still present. Also, if any router in a network segment uses a secondary address, all other routers in that segment must also use a secondary address from the same network or subnet address space.

- If **bootp** or **dhcp** options are selected, the system will immediately start broadcasting service requests for all VLANs configured to obtain address assignments through BOOTP or DHCP. IP is enabled but will not function until a BOOTP or DHCP reply has been received. Requests are broadcast periodically by the router in an effort to learn its IP address. (BOOTP and DHCP values can include the IP address, default gateway, and subnet mask). If the DHCP/BOOTP server is slow to respond, you may need to use the ip dhcp restart client command to re-start broadcasting service requests, or reboot the router.

**NOTE:** Each VLAN group can be assigned its own IP interface address. Therefore, if routing is enabled, you can manage the router via any of these IP addresses.

### EXAMPLE

In the following example, the device is assigned an address in VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

### RELATED COMMANDS

ip dhcp restart client (1040)
ipv6 address (1083)

## ip default-gateway

This command specifies the default gateway for destinations not found in the local routing tables. Use the **no** form to remove a default gateway.

### SYNTAX

**ip default-gateway** *gateway*

**no ip default-gateway**

*gateway* - IP address of the default gateway

### DEFAULT SETTING
No default gateway is established.

### COMMAND MODE
Global Configuration

### COMMAND USAGE
- The default gateway can also be defined using the following command:
  **ip route 0.0.0.0 0.0.0.0** *gateway-address*.

- Static routes can also be defined using the ip route command to ensure that traffic to the designated address or subnet passes through a preferred gateway.

- A default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the router.

- The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address for a default gateway, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface from which the ping is sent.

### EXAMPLE
The following example defines a default gateway for this device:

```
Console(config)#ip default-gateway 10.1.1.254
Console(config)#end
Console#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*     0.0.0.0/0 [1/0] via 10.1.1.254, VLAN1
C      127.0.0.0/8 is directly connected, lo0
C      192.168.2.0/24 is directly connected, VLAN1
```

### RELATED COMMANDS
ip route (1114)
show ip route (1115)
ipv6 default-gateway (1082)

## show ip interface

This command displays the settings of an IPv4 interface.

#### COMMAND MODE

Privileged Exec

#### EXAMPLE

```
Console#show ip interface
Loopback 0 is Administrative Up - Link Up
  Address is 00-00-00-00-00-00
  Index: 746, MTU: 0
  Address Mode is User specified
  Proxy ARP is disabled
Vlan 1 is Administrative Up - Link Up
  Address is 00-00-E8-93-82-A0 (via 00-00-E8-93-82-A0)
  Index: 1001, MTU: 1280, Bandwidth: 1g
  Address Mode is User specified
  IP Address: 192.168.1.3 Mask: 255.255.255.0
  Proxy ARP is disabled
Console#
```

#### RELATED COMMANDS

ip address (1068)
show ip redirects (367)
show ipv6 interface (1089)

## traceroute

This command shows the route packets take to the specified destination.

#### SYNTAX

**traceroute** *host*

*host* - IP address or alias of the host.

#### DEFAULT SETTING

None

#### COMMAND MODE

Privileged Exec

#### COMMAND USAGE

- Use the **traceroute** command to determine the path taken to reach a specified destination.
- A trace terminates when the destination responds, when the maximum timeout (TTL) is exceeded, or the maximum number of hops is exceeded.
- The traceroute command first sends probe datagrams with the TTL value set at one. This causes the first router to discard the datagram and return an error message. The trace function then sends several probe messages at each subsequent TTL level and displays the round-trip time for each message. Not all devices respond correctly to probes by returning an “ICMP port unreachable” message. If the timer goes off before a response is returned, the trace function

prints a series of asterisks and the “Request Timed Out” message. A long sequence of these messages, terminating only when the maximum timeout has been reached, may indicate this problem with the target device.

### Example

```
Console#traceroute 192.168.0.1
Press "ESC" to abort.

Source address:       192.168.0.9
Destination address:   192.168.0.1

Hop    IP Address           Packet 1          Packet 2          Packet 3
---------------------------------------------------------------------------
1    192.168.0.1              <10 ms            <10 ms            <10 ms

Trace completed.
Console#
```

## ping

This command sends (IPv4) ICMP echo request packets to another node on the network.

### Syntax

**ping** *host* [**count** *count*] [**size** *size*]

*host* - IP address or IP alias of the host.

*count* - Number of packets to send. (Range: 1-16)

*size* - Number of bytes in a packet. (Range: 32-512)
The actual packet size will be eight bytes larger than the size specified because the router adds header information.

### Default Setting

count: 5
size: 32 bytes

### Command Mode

Normal Exec, Privileged Exec

### Command Usage

- Use the ping command to see if another site on the network can be reached.

- The following are some results of the **ping** command:

  - *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.

  - *Destination does not respond* - If the host does not respond, a “timeout” appears in ten seconds.

  - *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.

- *Network or host unreachable* - The gateway found no corresponding entry in the route table.

- When pinging a host name, be sure the DNS server has been enabled (see page 1032). If necessary, local devices can also be specified in the DNS static host table (see page 1034).

### EXAMPLE

```
Console#ping 10.1.0.9
Type ESC to abort.
PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 5 seconds
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 0 ms
Ping statistics for 10.1.0.9:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
 Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms
Console#
```

### RELATED COMMANDS

interface (806)

## ARP CONFIGURATION

This section describes commands used to configure the Address Resolution Protocol (ARP) on the switch.

**Table 4: Address Resolution Protocol Commands**

| Command | Function | Mode |
|---|---|---|
| arp | Adds a static entry in the ARP cache | GC |
| arp timeout | Sets the time a dynamic entry remains in the ARP cache | GC |
| ip proxy-arp | Enables proxy ARP service | IC |
| clear arp-cache | Deletes all dynamic entries from the ARP cache | PE |
| show arp | Displays entries in the ARP cache | NE, PE |

## arp

This command adds a static entry in the Address Resolution Protocol (ARP) cache. Use the **no** form to remove an entry from the cache.

### SYNTAX

**arp** *ip-address hardware-address*

**no arp** *ip-address*

*ip-address* - IP address to map to a specified hardware address.

*hardware-address* - Hardware address to map to a specified IP address. (The format for this address is xx-xx-xx-xx-xx-xx.)

**DEFAULT SETTING**
No default entries

**COMMAND MODE**
Global Configuration

**COMMAND USAGE**

- The ARP cache is used to map 32-bit IP addresses into 48-bit hardware (i.e., Media Access Control) addresses. This cache includes entries for hosts and other routers on local network interfaces defined on this router.

- The maximum number of static entries allowed in the ARP cache is 128.

- You may need to enter a static entry in the cache if there is no response to an ARP broadcast message. For example, some applications may not respond to ARP requests or the response arrives too late, causing network operations to time out.

- Static entries will not be aged out nor deleted when power is reset. A static entry can only be removed through the configuration interface.

**EXAMPLE**

```
Console(config)#arp 10.1.0.19 01-02-03-04-05-06
Console(config)#
```

**RELATED COMMANDS**
clear arp-cache (1076)
show arp (1076)

## arp timeout

This command sets the aging time for dynamic entries in the Address Resolution Protocol (ARP) cache. Use the **no** form to restore the default timeout.

**SYNTAX**

**arp timeout** *seconds*

**no arp timeout**

*seconds* - The time a dynamic entry remains in the ARP cache. (Range: 300-86400; 86400 seconds is one day)

**DEFAULT SETTING**
1200 seconds (20 minutes)

**COMMAND MODE**
Global Configuration

**COMMAND USAGE**

- When a ARP entry expires, it is deleted from the cache and an ARP request packet is sent to re-establish the MAC address.

- The aging time determines how long dynamic entries remain in the cache. If the timeout is too short, the router may tie up resources by repeating ARP requests for addresses recently flushed from the table.

#### EXAMPLE

This example sets the ARP cache timeout for 15 minutes (i.e., 900 seconds).

```
Console(config)#arp timeout 900
Console(config)#
```

### ip proxy-arp

This command enables proxy Address Resolution Protocol (ARP). Use the **no** form to disable proxy ARP.

#### SYNTAX

[**no**] **ip proxy-arp**

#### DEFAULT SETTING

Disabled

#### COMMAND MODE

Interface Configuration (VLAN)

#### COMMAND USAGE

- Proxy ARP allows a non-routing device to determine the MAC address of a host on another subnet or network.

- End stations that require Proxy ARP must view the entire network as a single network. These nodes must therefore use a smaller subnet mask than that used by the router or other relevant network devices.

- Extensive use of Proxy ARP can degrade router performance because it may lead to increased ARP traffic and increased search time for larger ARP address tables.

#### EXAMPLE

```
Console(config)#interface vlan 3
Console(config-if)#ip proxy-arp
Console(config-if)#
```

## clear arp-cache

This command deletes all dynamic entries from the Address Resolution Protocol (ARP) cache.

### COMMAND MODE

Privileged Exec

### EXAMPLE

This example clears all dynamic entries in the ARP cache.

```
Console#clear arp-cache
This operation will delete all the dynamic entries in ARP Cache.
Are you sure to continue this operation (y/n)?y
Console#
```

## show arp

This command displays entries in the Address Resolution Protocol (ARP) cache.

### COMMAND MODE

Normal Exec, Privileged Exec

### COMMAND USAGE

This command displays information about the ARP cache. The first line shows the cache timeout. It also shows each cache entry, including the IP address, MAC address, type (static, dynamic, other), and VLAN interface. Note that entry type “other” indicates local addresses for this router.

### EXAMPLE

This example displays all entries in the ARP cache.

```
Console#show arp
Arp cache timeout: 1200 (seconds)

IP Address      MAC Address       Type      Interface
--------------- ----------------- --------- -----------
       10.1.0.0 ff-ff-ff-ff-ff-ff     other VLAN 1
     10.1.0.254 00-00-ab-cd-00-00     other VLAN 1
     10.1.0.255 ff-ff-ff-ff-ff-ff     other VLAN 1
  123.20.10.123 02-10-20-30-40-50    static VLAN 2
   345.30.20.23 09-50-40-30-20-10   dynamic VLAN 3

Total entry : 5
Console#
```

## UDP HELPER CONFIGURATION

User Datagram Protocol (UDP) Helper allows host applications to forward UDP broadcast packets from this switch to another part of the network. This section describes the commands used to configure UDP Helper.

**Table 5: UDP Helper Commands**

| Command | Function | Mode |
|---|---|---|
| ip forward-protocol udp | Specifies the UDP destination ports for which broadcast traffic will be forwarded | GC |
| ip helper | Enables UDP helper globally on the switch | GC |
| ip helper-address | Specifies the servers to which designated UDP protocol packets are forwarded | IC |
| show ip helper | Displays configuration settings for UDP helper | PE |

## ip forward-protocol udp

This command specifies the UDP destination ports for which broadcast traffic will be forwarded when the UDP helper is enabled. Use the **no** form to remove a UDP port from the forwarding list.

### SYNTAX

[**no**] **ip forward-protocol udp** *destination-port*

*destination-port* - UDP application port for which UDP service requests are forwarded. (Range: 1-65535)

### DEFAULT SETTING

The following UDP ports are included in the forwarding list when UDP helper is enabled with the ip helper command, and a remote server address is configured with the ip helper-address command:

BOOTP client port 67
BOOTP server port 68
Domain Name Service port 53
IEN-116 Name Service port 42
NetBIOS Datagram Server port 138
NetBIOS Name Server port 137
NTP port 37
TACACS service port 49
TFTP port 69

### COMMAND MODE

Global Configuration

### COMMAND USAGE

Up to 100 UDP ports can be specified with this command for forwarding to one or more remote servers.

#### EXAMPLE

This example enables forwarding for DHCPv6 UDP packets.

```
Console(config)#ip forward-protocol udp 547
Console(config)#
```

## ip helper

This command enables UDP helper globally on the switch. Use the **no** form to disable this feature.

#### SYNTAX

[**no**] **ip helper**

#### DEFAULT SETTING

Disabled

#### COMMAND MODE

Global Configuration

#### COMMAND USAGE

- Network hosts occasionally use UDP broadcasts to determine information such as address configuration, and domain name mapping. These broadcasts are confined to the local subnet, either as an all hosts broadcast (all ones broadcast - 255.255.255.255), or a directed subnet broadcast (such as 10.10.10.255). To reduce the number of application servers deployed in a multi-segment network, UDP helper can be used to forward broadcast packets for specified UDP application ports to remote servers located in another network segment.

- To configure UDP helper, it must be enabled globally with the **ip helper** command. The UDP destination ports for which broadcast traffic will be forwarded must be specified with the ip forward-protocol udp command. And the remote servers which are configured to service UDP clients on another network segment specified with the ip helper-address command.

#### EXAMPLE

This example enables UDP helper globally on the switch.

```
Console(config)#ip helper
Console(config)#
```

## ip helper-address

This command specifies the application server or subnet (indicated by a directed broadcast address) to which designated UDP broadcast packets are forwarded. Use the **no** form to remove a UDP helper address.

### SYNTAX

[**no**] **ip helper-address** *ip-address*

*ip-address* - Host address or directed broadcast address to which UDP broadcast packets are forwarded. (Range: 1-65535)

### DEFAULT SETTING

None

### COMMAND MODE

Interface Configuration (VLAN)

### COMMAND USAGE

- Up to 20 helper addresses can be specified with this command.
- To forward UDP packets with the UDP helper, the clients must be connected to the selected interface, and the interface configured with an IP address.
- The UDP packets to be forwarded must be specified by the ip forward-protocol udp command, and the packets meet the following criteria:
  - The MAC address of the received frame must be all-ones broadcast address (ffff.ffff.ffff).
  - The IP destination address must be one of the following:
    - all-ones broadcast (255.255.255.255)
    - subnet broadcast for the receiving interface
  - The IP time-to-live (TTL) value must be at least 2.
  - The IP protocol must be UDP (17).
  - The UDP destination port must be TFTP, Domain Name System (DNS), Time, NetBIOS, BOOTP or DHCP packet, or a UDP port specified by the ip forward-protocol udp command.
- If a helper address is specified with this command, but no UDP ports have been specified with the ip forward-protocol udp command, broadcast traffic for several UDP protocol types will be forwarded by default as described under the ip forward-protocol udp command.

#### EXAMPLE

This example indicates that designated UDP broadcast packets are to be forwarded to the directed broadcast address of 192.168.2.255.

```
Console(config)#interface vlan 1
Console(config-if)#ip helper-address 192.168.2.255
Console(config-if)#
```

## show ip helper

This command displays configuration settings for UDP helper.

#### COMMAND MODE

Privileged Exec

#### COMMAND USAGE

This command displays all configuration settings for UDP helper, including its functional status, the UDP ports for which broadcast traffic will be forwarded, and the remote servers or subnets to which the traffic will be forwarded.

#### EXAMPLE

```
Console#show ip helper
Helper mechanism is enabled
Forward port list(maximum count: 100)
  547
Total port number now is: 1
Helper address list(maximum count: 1024)
Interface vlan 1:
  192.168.1.44
  192.168.2.255
Total helper number now is: 2
Console#
```

# IPV6 INTERFACE

This switch supports the following IPv6 interface commands.

**Table 6: IPv6 Configuration Commands**

| Command | Function | Mode |
|---|---|---|
| *Interface Address Configuration and Utilities* | | |
| ipv6 default-gateway | Sets an IPv6 default gateway for traffic with no known next hop | GC |
| ipv6 address | Configures an IPv6 global unicast address, and enables IPv6 on an interface | IC |
| ipv6 address eui-64 | Configures an IPv6 global unicast address for an interface using an EUI-64 interface ID in the low order 64 bits, and enables IPv6 on the interface | IC |
| ipv6 address link-local | Configures an IPv6 link-local address for an interface and enables IPv6 on the interface | IC |
| ipv6 enable | Enables IPv6 on an interface that has not been configured with an explicit IPv6 address | IC |
| ipv6 mtu | Sets the size of the maximum transmission unit (MTU) for IPv6 packets sent on an interface | IC |
| show ipv6 interface | Displays the usability and configured settings for IPv6 interfaces | NE, PE |
| show ipv6 mtu | Displays maximum transmission unit (MTU) information for IPv6 interfaces | NE, PE |
| show ipv6 traffic | Displays statistics about IPv6 traffic | NE, PE |
| clear ipv6 traffic | Resets IPv6 traffic counters | PE |
| ping6 | Sends IPv6 ICMP echo request packets to another node on the network | PE |
| *Neighbor Discovery* | | |
| ipv6 hop-limit | Configures the maximum number of hops used in router advertisements that are originated by this router | GC |
| ipv6 neighbor | Configures a static entry in the IPv6 neighbor discovery cache | GC |
| ipv6 nd dad attempts | Configures the number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection | IC |
| ipv6 nd ns-interval | Configures the interval between IPv6 neighbor solicitation retransmissions on an interface | IC |
| ipv6 nd reachable-time | Configures the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred | IC |
| clear ipv6 neighbors | Deletes all dynamic entries in the IPv6 neighbor discovery cache | PE |
| show ipv6 neighbors | Displays information in the IPv6 neighbor discovery cache | PE |

## ipv6 default-gateway

This command sets an IPv6 default gateway to use for destinations with no known next hop. Use the **no** form to remove a previously configured default gateway.

### Syntax

**ipv6 default-gateway** *ipv6-address*

**no ipv6 address**

*ipv6-address* - The IPv6 address of the default next hop router to use for destinations with no known next hop.

### Default Setting

No default gateway is defined

### Command Mode

Global Configuration

### Command Usage

- All IPv6 addresses must be according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

- The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface from which the ping is sent.

- An IPv6 default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the switch.

### Example

The following example defines a default gateway for this device:

```
Console(config)#ipv6 default-gateway 2001:DB8:2222:7272::254
Console(config)#
```

### Related Commands

show ipv6 route (1119)
ip default-gateway (1069)

## ipv6 address

This command configures an IPv6 global unicast address and enables IPv6 on an interface. Use the **no** form without any arguments to remove all IPv6 addresses from the interface, or use the **no** form with a specific IPv6 address to remove that address from the interface.

### SYNTAX

**ipv6 address** *ipv6-address*/*prefix-length*

**no ipv6 address** [*ipv6-address*/*prefix-length*]

*ipv6-address* - A full IPv6 address including the network prefix and host address bits.

*prefix-length* - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

### DEFAULT SETTING

No IPv6 addresses are defined

### COMMAND MODE

Interface Configuration (VLAN, IPv6/v4 Tunnel)

### COMMAND USAGE

- All IPv6 addresses must be according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

- To connect to a larger network with multiple subnets, you must configure a global unicast address. This address can be manually configured with this command.

- If a link-local address has not yet been assigned to this interface, this command will assign the specified static global unicast address and also dynamically generate a link-local unicast address for the interface. (The link-local address is made with an address prefix of FE80 and a host portion based the switch’s MAC address in modified EUI-64 format.)

- When configuring an global IPv6 address for a static tunnel, the link-local address generated by this command is the 32-bit IPv4 address of the underlying source interface, with the bytes in the same order in which they would appear in the header of an IPv4 packet, padded at the left with zeros to a total of 64 bits. Note that the “Universal/Local” bit is zero, indicating that the interface identifier is not globally unique. When the host has more than one IPv4 address in use on the physical interface concerned, the primary address for that interface is used. The IPv6 link-local address for an IPv4 virtual interface is formed by appending the interface identifier, as defined above, to the prefix FE80::/64.

- If a duplicate address is detected, a warning message is sent to the console.

### EXAMPLE

This example specifies a full IPv6 address and prefix length.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2001:DB8:2222:7272::72/96
Console(config-if)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::2E0:CFF:FE00:FD/64
Global unicast address(es):
  2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96
Joined group address(es):
FF02::1:FF00:72
FF02::1:FF00:FD
FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds

Console#
```

### RELATED COMMANDS

ipv6 address eui-64 (1084)
show ipv6 interface (1089)
ip address (1068)

## ipv6 address eui-64

This command configures an IPv6 address for an interface using an EUI-64 interface ID in the low order 64 bits and enables IPv6 on the interface. Use the **no** form without any arguments to remove all manually configured IPv6 addresses from the interface. Use the **no** form with a specific address to remove it from the interface.

### SYNTAX

**ipv6 address** *ipv6-prefix*/*prefix-length* **eui-64**

**no ipv6 address** [*ipv6-prefix*/*prefix-length* **eui-64**]

*ipv6-prefix* - The IPv6 network portion of the address assigned to the interface.

*prefix-length* - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

### DEFAULT SETTING

No IPv6 addresses are defined

### COMMAND MODE

Interface Configuration (VLAN, IPv6/v4 Tunnel)

### COMMAND USAGE

- The prefix must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

- If a link local address has not yet been assigned to this interface, this command will dynamically generate a global unicast address and a link-local address for this interface. (The link-local address is made with an address prefix of FE80 and a host portion based the switch's MAC address in modified EUI-64 format.)

- Note that the value specified in the ipv6-prefix may include some of the high-order host bits if the specified prefix length is less than 64 bits. If the specified prefix length exceeds 64 bits, then the network portion of the address will take precedence over the interface identifier.

- If a duplicate address is detected, a warning message is sent to the console.

- IPv6 addresses are 16 bytes long, of which the bottom 8 bytes typically form a unique host identifier based on the device's MAC address. The EUI-64 specification is designed for devices that use an extended 8-byte MAC address. For devices that still use a 6-byte MAC address (also known as EUI-48 format), it must be converted into EUI-64 format by inverting the universal/local bit in the address and inserting the hexadecimal number FFFE between the upper and lower three bytes of the MAC address.

- For example, if a device had an EUI-48 address of 28-9F-18-1C-82-35, the global/ local bit must first be inverted to meet EUI-64 requirements (i.e., 1 for globally defined addresses and 0 for locally defined addresses), changing 28 to 2A. Then the two bytes FFFE are inserted between the OUI (i.e., company id) and the rest of the address, resulting in a modified EUI-64 interface identifier of 2A-9F-18-FF-FE-1C-82-35.

- This host addressing method allows the same interface identifier to be used on multiple IP interfaces of a single device, as long as those interfaces are attached to different subnets.

- When configuring an global IPv6 address for a static tunnel, the link-local address generated by this command is the 32-bit IPv4 address of the underlying source interface, with the bytes in the same order in which they would appear in the header of an IPv4 packet, padded at the left with zeros to a total of 64 bits. Note that the "Universal/Local" bit is zero, indicating that the interface identifier is not globally unique. When the host has more than one IPv4 address in use on the physical interface concerned, the primary address for that interface is used. The IPv6 link-local address for an IPv4 virtual interface is formed by appending the interface identifier, as defined above, to the prefix FE80::/64.

### EXAMPLE

This example uses the network prefix of 2001:0DB8:0:1::/64, and specifies that the EUI-64 interface identifier be used in the lower 64 bits of the address.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2001:0DB8:0:1::/64 eui-64
Console(config-if)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
```

```
  FE80::2E0:CFF:FE00:FD/64
Global unicast address(es):
  2001:DB8::1:2E0:CFF:FE00:FD/64, subnet is 2001:DB8::1:0:0:0:0/64[EUI]
  2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96[EUI]
Joined group address(es):
FF02::1:FF00:72
FF02::1:FF00:FD
FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds

Console#
```

### Related Commands

show ipv6 interface (1089)

## ipv6 address link-local

This command configures an IPv6 link-local address for an interface and enables IPv6 on the interface. Use the **no** form without any arguments to remove all manually configured IPv6 addresses from the interface. Use the **no** form with a specific address to remove it from the interface.

### Syntax

**ipv6 address** *ipv6-address* **link-local**

**no ipv6 address** [*ipv6-address* **link-local**]

*ipv6-address* - The IPv6 address assigned to the interface.

### Default Setting

No IPv6 addresses are defined

### Command Mode

Interface Configuration (VLAN, IPv6/v4 Tunnel)

### Command Usage

- The specified address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. And the address prefix must be FE80.

- The address specified with this command replaces a link-local address that was automatically generated for the interface.

- You can configure multiple IPv6 global unicast addresses per interface, but only one link-local address per interface.

- If a duplicate address is detected, a warning message is sent to the console.

### Example

This example assigns a link-local address of FE80::269:3EF9:FE19:6779 to VLAN 1. Note that the prefix FE80 is required for link-local addresses, and the first 16-bit group in the host address is padded with a zero in the form 0269.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address FE80::269:3EF9:FE19:6779 link-local
Console(config-if)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::269:3EF9:FE19:6779/64
Global unicast address(es):
  2001:DB8::1:2E0:CFF:FE00:FD/64, subnet is 2001:DB8::1:0:0:0:0/64[EUI]
  2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96[EUI]
Joined group address(es):
FF02::1:FF19:6779
FF02::1:FF00:72
FF02::1:FF00:FD
FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds

Console#
```

### RELATED COMMANDS

ipv6 enable (1087)
show ipv6 interface (1089)

## ipv6 enable

This command enables IPv6 on an interface that has not been configured with an explicit IPv6 address. Use the **no** form to disable IPv6 on an interface that has not been configured with an explicit IPv6 address.

### SYNTAX

[no] ipv6 enable

### DEFAULT SETTING

IPv6 is disabled

### COMMAND MODE

Interface Configuration (VLAN)

### COMMAND USAGE

- This command enables IPv6 on the current VLAN interface and automatically generates a link-local unicast address. The address prefix uses FE80, and the host portion of the address is generated by converting the switch's MAC address to modified EUI-64 format (see page 1084). This address type makes the switch accessible over IPv6 for all devices attached to the same local subnet.
- If a duplicate address is detected on the local segment, this interface will be disabled and a warning message displayed on the console.
- The **no ipv6 enable** command does not disable IPv6 for an interface that has been explicitly configured with an IPv6 address.

### EXAMPLE

In this example, IPv6 is enabled on VLAN 1, and the link-local address FE80::2E0:CFF:FE00:FD/64 is automatically generated by the switch.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 enable
Console(config-if)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::200:E8FF:FE93:82A0/64
Global unicast address(es):
  2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96
Joined group address(es):
FF02::1:2
FF02::1:FF00:72
FF02::1:FF00:0
FF02::1:FF93:82A0
FF02::1
IPv6 link MTU is 1280 bytes
ND DAD is enabled, number of DAD attempts: 2.
ND retransmit interval is 1000 milliseconds

Console#
```

### RELATED COMMANDS

ipv6 address link-local (1086)
show ipv6 interface (1089)

## ipv6 mtu

This command sets the size of the maximum transmission unit (MTU) for IPv6 packets sent on an interface. Use the **no** form to restore the default setting.

### SYNTAX

**ipv6 mtu** *size*

**no ipv6 mtu**

*size* - Specifies the MTU size. (Range: 1280-65535 bytes)

### DEFAULT SETTING

1500 bytes

### COMMAND MODE

Interface Configuration (VLAN)

### COMMAND USAGE

- The maximum value set by this command cannot exceed the MTU of the physical interface, which is currently fixed at 1500 bytes.
- If a non-default value is configured, an MTU option is included in the router advertisements sent from this device.

■IPv6 routers do not fragment IPv6 packets forwarded from other routers. However, traffic originating from an end-station connected to an IPv6 router may be fragmented.

■All devices on the same physical medium must use the same MTU in order to operate correctly.

■IPv6 must be enabled on an interface before the MTU can be set.

### EXAMPLE

The following example sets the MTU for VLAN 1 to 1280 bytes:

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 mtu 1280
Console(config-if)#
```

### RELATED COMMANDS

show ipv6 mtu (1091)
jumbo frame (622)

## show ipv6 interface

This command displays the usability and configured settings for IPv6 interfaces.

### SYNTAX

**show ipv6 interface** [**brief** [**vlan** *vlan-id* [*ipv6-prefix*/*prefix-length*]]]

**brief** - Displays a brief summary of IPv6 operational status and the addresses configured for each interface.

*vlan-id* - VLAN ID (Range: 1-4093)

*ipv6-prefix* - The IPv6 network portion of the address assigned to the interface. The prefix must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

*prefix-length* - A decimal value indicating how many of the contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

### COMMAND MODE

Normal Exec, Privileged Exec

### EXAMPLE

This example displays all the IPv6 addresses configured for the switch.

```
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::200:E8FF:FE93:82A0/64
Global unicast address(es):
```

```
  2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96
Joined group address(es):
FF02::1:2
FF02::1:FF00:72
FF02::1:FF00:0
FF02::1:FF93:82A0
FF02::1
IPv6 link MTU is 1280 bytes
ND DAD is enabled, number of DAD attempts: 2.
ND retransmit interval is 1000 milliseconds

Console#
```

**Table 7: show ipv6 interface** - display description

| Field | Description |
| --- | --- |
| VLAN | A VLAN is marked “up” if the switch can send and receive packets on this interface, “down” if a line signal is not present, or “administratively down” if the interface has been disabled by the administrator. |
| IPv6 | IPv6 is marked “enable” if the switch can send and receive IP traffic on this interface, “disable” if the switch cannot send and receive IP traffic on this interface, or “stalled” if a duplicate link-local address is detected on the interface. |
| Link-local address | Shows the link-local address assigned to this interface |
| Global unicast address(es) | Shows the global unicast address(es) assigned to this interface |
| Joined group address(es) | In addition to the unicast addresses assigned to an interface, a node is required to join the all-nodes multicast addresses FF01::1 and FF02::1 for all IPv6 nodes within scope 1 (interface-local) and scope 2 (link-local), respectively.<br>FF01::1/16 is the transient node-local multicast address for all attached IPv6 nodes, and FF02::1/16 is the link-local multicast address for all attached IPv6 nodes. The node-local multicast address is only used for loopback transmission of multicast traffic. Link-local multicast addresses cover the same types as used by link-local unicast addresses, including all nodes (FF02::1), all routers (FF02::2), and solicited nodes (FF02::1:FFXX:XXXX) as described below.<br>A node is also required to compute and join the associated solicited-node multicast addresses for every unicast and anycast address it is assigned. IPv6 addresses that differ only in the high-order bits, e.g. due to multiple high-order prefixes associated with different aggregations, will map to the same solicited-node address, thereby reducing the number of multicast addresses a node must join. In this example, FF02::1:FF90:0/104 is the solicited-node multicast address which is formed by taking the low-order 24 bits of the address and appending those bits to the prefix. |
| MTU | Maximum transmission unit for this interface. |
| ND DAD | Indicates whether (neighbor discovery) duplicate address detection is enabled. |
| number of DAD attempts | The number of consecutive neighbor solicitation messages sent on the interface during duplicate address detection. |
| ND retransmit interval | The interval between IPv6 neighbor solicitation retransmissions sent on an interface during duplicate address detection. |

This example displays a brief summary of IPv6 addresses configured on the switch.

```
Console#show ipv6 interface brief
Interface      VLAN       IPv6      IPv6 Address
--------------- ---------- ---------- ---------------------------------------
VLAN 1         Up         Up        2001:DB8:2222:7272::72/96
VLAN 1         Up         Up        FE80::200:E8FF:FE93:82A0%1/64
Console#
```

### RELATED COMMANDS

show ip interface (1071)

## show ipv6 mtu

This command displays the maximum transmission unit (MTU) cache for destinations that have returned an ICMP packet-too-big message along with an acceptable MTU to this switch.

### COMMAND MODE

Normal Exec, Privileged Exec

### EXAMPLE

The following example shows the MTU cache for this device:

```
Console#show ipv6 mtu
MTU    Since   Destination Address
1400   00:04:21  5000:1::3
1280   00:04:50  FE80::203:A0FF:FED6:141D
Console#
```

**Table 8: show ipv6 mtu** - display description

| Field | Description |
|---|---|
| MTU | Adjusted MTU contained in the ICMP packet-too-big message returned from this destination, and now used for all traffic sent along this path. |
| Since | Time since an ICMP packet-too-big message was received from this destination. |
| Destination Address | Address which sent an ICMP packet-too-big message. |

## show ipv6 traffic

This command displays statistics about IPv6 traffic passing through this switch.

### COMMAND MODE

Normal Exec, Privileged Exec

### EXAMPLE

The following example shows statistics for all IPv6 unicast and multicast traffic, as well as ICMP, UDP and TCP statistics:

```
Console#show ipv6 traffic
IPv6 Statistics:
IPv6 received
          total received
          header errors
          too big errors
          no routes
          address errors
          unknown protocols
          truncated packets
          discards
          delivers
          reassembly request datarams
```

```
                    reassembled succeeded
                    reassembled failed
IPv6 sent
                    forwards datagrams
                 15 requests
                    discards
                    no routes
                    generated fragments
                    fragment succeeded
                    fragment failed
ICMPv6 Statistics:
ICMPv6 received
                    input
                    errors
                    destination unreachable messages
                    packet too big messages
                    time exceeded messages
                    parameter problem message
                    echo request messages
                    echo reply messages
                    router solicit messages
                    router advertisement messages
                    neighbor solicit messages
                    neighbor advertisement messages
                    redirect messages
                    group membership query messages
                    group membership response messages
                    group membership reduction messages
                    multicast listener discovery version 2 reports
ICMPv6 sent
                 15 output
                    destination unreachable messages
                    packet too big messages
                    time exceeded messages
                    parameter problem message
                    echo request messages
                    echo reply messages
                  7 router solicit messages
                    router advertisement messages
                  3 neighbor solicit messages
                    neighbor advertisement messages
                    redirect messages
                    group membership query messages
                    group membership response messages
                    group membership reduction messages
                    multicast listener discovery version 2 reports
UDP Statistics:
                    input
                    no port errors
                    other errors
                    output
Console#
```

**Table 9: show ipv6 traffic** - display description

| Field | Description |
|---|---|
| *IPv6 Statistics* | |
| *IPv6 received* | |
| total received | The total number of input datagrams received by the interface, including those received in error. |

**Table 9: show ipv6 traffic** - display description (Continued)

| Field | Description |
|---|---|
| header errors | The number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, IPv6 options, etc. |
| too big errors | The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface. |
| no routes | The number of input datagrams discarded because no route could be found to transmit them to their destination. |
| address errors | The number of input datagrams discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., ::0) and unsupported addresses (e.g., addresses with unallocated prefixes). For entities which are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address. |
| unknown protocols | The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams. |
| truncated packets | The number of input datagrams discarded because datagram frame didn't carry enough data. |
| discards | The number of input IPv6 datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly. |
| delivers | The total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams. |
| reassembly request datagrams | The number of IPv6 fragments received which needed to be reassembled at this interface. Note that this counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments. |
| reassembled succeeded | The number of IPv6 datagrams successfully reassembled. Note that this counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the fragments. |
| reassembled failed | The number of failures detected by the IPv6 re-assembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received. This counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments. |
| *IPv6 sent* | |
| forwards datagrams | The number of output datagrams which this entity received and forwarded to their final destinations. In entities which do not act as IPv6 routers, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route processing was successful. Note that for a successfully forwarded datagram the counter of the outgoing interface is incremented. |
| requests | The total number of IPv6 datagrams which local IPv6 user-protocols (including ICMP) supplied to IPv6 in requests for transmission. Note that this counter does not include any datagrams counted in ipv6IfStatsOutForwDatagrams. |
| discards | The number of output IPv6 datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipv6IfStatsOutForwDatagrams if any such packets met this (discretionary) discard criterion. |

**Table 9: show ipv6 traffic** - display description (Continued)

| Field | Description |
|---|---|
| no routes | The number of input datagrams discarded because no route could be found to transmit them to their destination. |
| generated fragments | The number of output datagram fragments that have been generated as a result of fragmentation at this output interface. |
| fragment succeeded | The number of IPv6 datagrams that have been successfully fragmented at this output interface. |
| fragment failed | The number of IPv6 datagrams that have been discarded because they needed to be fragmented at this output interface but could not be. |
| *ICMPv6 Statistics* | |
| *ICMPv6 received* | |
| input | The total number of ICMP messages received by the interface which includes all those counted by ipv6IfIcmpInErrors. Note that this interface is the interface to which the ICMP messages were addressed which may not be necessarily the input interface for the messages. |
| errors | The number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.). |
| destination unreachable messages | The number of ICMP Destination Unreachable messages received by the interface. |
| packet too big messages | The number of ICMP Packet Too Big messages received by the interface. |
| time exceeded messages | The number of ICMP Time Exceeded messages received by the interface. |
| parameter problem message | The number of ICMP Parameter Problem messages received by the interface. |
| echo request messages | The number of ICMP Echo (request) messages received by the interface. |
| echo reply messages | The number of ICMP Echo Reply messages received by the interface. |
| router solicit messages | The number of ICMP Router Solicit messages received by the interface. |
| router advertisement messages | The number of ICMP Router Advertisement messages received by the interface. |
| neighbor solicit messages | The number of ICMP Neighbor Solicit messages received by the interface. |
| neighbor advertisement messages | The number of ICMP Neighbor Advertisement messages received by the interface. |
| redirect messages | The number of Redirect messages received by the interface. |
| group membership query messages | The number of ICMPv6 Group Membership Query messages received by the interface. |
| group membership response messages | The number of ICMPv6 Group Membership Response messages received by the interface. |
| group membership reduction messages | The number of ICMPv6 Group Membership Reduction messages received by the interface. |
| multicast listener discovery version 2 reports | The number of MLDv2 reports received by the interface. |
| *ICMPv6 sent* | |
| output | The total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors. |
| destination unreachable messages | The number of ICMP Destination Unreachable messages sent by the interface. |
| packet too big messages | The number of ICMP Packet Too Big messages sent by the interface. |

**Table 9: show ipv6 traffic** - display description (Continued)

| Field | Description |
|---|---|
| time exceeded messages | The number of ICMP Time Exceeded messages sent by the interface. |
| parameter problem message | The number of ICMP Parameter Problem messages sent by the interface. |
| echo request messages | The number of ICMP Echo (request) messages sent by the interface. |
| echo reply messages | The number of ICMP Echo Reply messages sent by the interface. |
| router solicit messages | The number of ICMP Router Solicitation messages sent by the interface. |
| router advertisement messages | The number of ICMP Router Advertisement messages sent by the interface. |
| neighbor solicit messages | The number of ICMP Neighbor Solicit messages sent by the interface. |
| neighbor advertisement messages | The number of ICMP Router Advertisement messages sent by the interface. |
| redirect messages | The number of Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects. |
| group membership query messages | The number of ICMPv6 Group Membership Query messages sent by the interface. |
| group membership response messages | The number of ICMPv6 Group Membership Response messages sent. |
| group membership reduction messages | The number of ICMPv6 Group Membership Reduction messages sent. |
| multicast listener discovery version 2 reports | The number of MLDv2 reports sent by the interface. |
| *UDP Statistics* | |
| input | The total number of UDP datagrams delivered to UDP users. |
| no port errors | The total number of received UDP datagrams for which there was no application at the destination port. |
| other errors | The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port. |
| output | The total number of UDP datagrams sent from this entity. |

## clear ipv6 traffic

This command resets IPv6 traffic counters.

### COMMAND MODE

Privileged Exec

### COMMAND USAGE

This command resets all of the counters displayed by the show ipv6 traffic command.

### EXAMPLE

```
Console#clear ipv6 traffic
Console#
```

**ping6** This command sends (IPv6) ICMP echo request packets to another node on the network.

### SYNTAX

**ping6** {*ipv6-address* | *host-name*} [**count** *count*] [**size** *size*]

*ipv6-address* - The IPv6 address of a neighbor device. You can specify either a link-local or global unicast address formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

*host-name* - A host name string which can be resolved into an IPv6 address through a domain name server.

*count* - Number of packets to send. (Range: 1-16)

*size* - Number of bytes in a packet. (Range: 48-18024 bytes)
The actual packet size will be eight bytes larger than the size specified because the router adds header information.

### DEFAULT SETTING

count: 5
size: 100 bytes

### COMMAND MODE

Privileged Exec

### COMMAND USAGE

- Use the **ping6** command to see if another site on the network can be reached, or to evaluate delays over the path.
- The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface from which the ping is sent.
- When pinging a host name, be sure the DNS server has been enabled (see page 1032). If necessary, local devices can also be specified in the DNS static host table (see page 1034).
- When using ping6 with a host name, the router first attempts to resolve the alias into an IPv6 address before trying to resolve it into an IPv4 address.

### EXAMPLE

```
Console#ping6 FE80::2E0:CFF:FE9C:CA10%1/64
Type ESC to abort.
PING to FE80::2E0:CFF:FE9C:CA10%1/64, by 5 0-byte payload ICMP packets, timeout is 3 seconds
response time: 20 ms    [FE80::2E0:CFF:FE9C:CA10]    seq_no: 1
response time: 0 ms     [FE80::2E0:CFF:FE9C:CA10]    seq_no: 2
response time: 10 ms    [FE80::2E0:CFF:FE9C:CA10]    seq_no: 3
response time: 0 ms     [FE80::2E0:CFF:FE9C:CA10]    seq_no: 4
response time: 10 ms    [FE80::2E0:CFF:FE9C:CA10]    seq_no: 5
Ping statistics for FE80::2E0:CFF:FE9C:CA10%1/64:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
```

```
Approximate round trip times:
 Minimum = 0 ms, Maximum = 20 ms, Average = 8 ms

Console#
```

## ipv6 neighbor

This command configures a static entry in the IPv6 neighbor discovery cache. Use the **no** form to remove a static entry from the cache.

### SYNTAX

**ipv6 neighbor** *ipv6-address* **vlan** *vlan-id hardware-address*

**no ipv6 mtu**

*ipv6-address* - The IPv6 address of a neighbor device that can be reached through one of the network interfaces configured on this switch. You can specify either a link-local or global unicast address formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

*vlan-id* - VLAN ID (Range: 1-4093)

*hardware-address* - The 48-bit MAC layer address for the neighbor device. This address must be formatted as six hexadecimal pairs separated by hyphens.

### DEFAULT SETTING

None

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- Address Resolution Protocol (ARP) has been replaced in IPv6 with the Neighbor Discovery Protocol (NDP). The **ipv6 neighbor** command is similar to the mac-address-table static command (page 854) that is implemented using ARP.

- Static entries can only be configured on an IPv6-enabled interface.

- The switch does not determine whether a static entry is reachable before placing it in the IPv6 neighbor discovery cache.

- If the specified entry was dynamically learned through the IPv6 neighbor discovery process, and already exists in the neighbor discovery cache, it is converted to a static entry. Static entries in the IPv6 neighbor discovery cache are not modified if subsequently detected by the neighbor discovery process.

- Disabling IPv6 on an interface with the no ipv6 enable command (see page 1087) deletes all dynamically learned entries in the IPv6 neighbor discovery cache for that interface, but does not delete static entries.

#### Example

The following maps a static entry for global unicast address to a MAC address:

```
Console(config)#ipv6 neighbor 2009:DB9:2229::81 vlan 1 30-65-14-01-11-86
Console(config)#end
Console#show ipv6 neighbors
State: I1 - Incomplete, I2 - Invalid, R - Reachable, S - Stale, D - Delay,
       P1 - Probe, P2 - Permanent, U - Unknown
IPv6 Address              Age        Link-layer Addr    State      VLAN
2009:DB9:2229::80         956        12-34-11-11-43-21      R         1
2009:DB9:2229::81         Permanent   30-65-14-01-11-86     R         1
FE80::1034:11FF:FE11:4321  961        12-34-11-11-43-21     R         1
Console#
```

#### Related Commands

show ipv6 neighbors (1102)
mac-address-table static (854)

### ipv6 hop-limit

This command configures the maximum number of hops used in router advertisements that are originated by this router. Use the **no** form to restore the default setting.

#### Syntax

**ipv6 hop-limit** *hops*

**no ipv6 hop-limit**

*hops* - The maximum number of hops in router advertisements and all IPv6 packets. (Range: 1-255)

#### Default Setting

1

#### Command Mode

Interface Configuration (VLAN)

#### Example

The following sets the hop limit for router advertisements to 64:

```
Console(config-if)#interface vlan 1
Console(config)#ipv6 hop-limit 64
Console(config)#
```

## ipv6 nd dad attempts

This command configures the number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection. Use the **no** form to restore the default setting.

### SYNTAX

**ipv6 nd dad attempts** *count*

**no ipv6 nd dad attempts**

*count* - The number of neighbor solicitation messages sent to determine whether or not a duplicate address exists on this interface. (Range: 0-600)

### DEFAULT SETTING

1

### COMMAND MODE

Interface Configuration (VLAN)

### COMMAND USAGE

- Configuring a value of 0 disables duplicate address detection.
- Duplicate address detection determines if a new unicast IPv6 address already exists on the network before it is assigned to an interface.
- Duplicate address detection is stopped on any interface that has been suspended (see the vlan command). While an interface is suspended, all unicast IPv6 addresses assigned to that interface are placed in a “pending” state. Duplicate address detection is automatically restarted when the interface is administratively re-activated.
- An interface that is re-activated restarts duplicate address detection for all unicast IPv6 addresses on the interface. While duplicate address detection is performed on the interface’s link-local address, the other IPv6 addresses remain in a “tentative” state. If no duplicate link-local address is found, duplicate address detection is started for the remaining IPv6 addresses.
- If a duplicate address is detected, it is set to “duplicate” state, and a warning message is sent to the console. If a duplicate link-local address is detected, IPv6 processes are disabled on the interface. If a duplicate global unicast address is detected, it is not used. All configuration commands associated with a duplicate address remain configured while the address is in “duplicate” state.
- If the link-local address for an interface is changed, duplicate address detection is performed on the new link-local address, but not for any of the IPv6 global unicast addresses already associated with the interface.

### EXAMPLE

The following configures five neighbor solicitation attempts for addresses configured on VLAN 1. The show ipv6 interface command indicates that the duplicate address detection process is still on-going.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 nd dad attempts 5
```

```
Console(config-if)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::2E0:CFF:FE9C:CA10/64
Global unicast address(es):
  2001:DB8:2222:7272::/64, subnet is 2001:DB8:2222:7272::/64
  2009:DB9:2229::79, subnet is ::
Joined group address(es):
FF02::2
FF02::1:FF00:0
FF02::1:2
FF02::1:FF9C:CA10
FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 5.
ND retransmit interval is 1000 milliseconds
Console#
```

### RELATED COMMANDS

ipv6 nd ns-interval (1100)
show ipv6 neighbors (1102)

## ipv6 nd ns-interval

This command configures the interval between transmitting IPv6 neighbor solicitation messages on an interface. Use the **no** form to restore the default value.

### SYNTAX

**ipv6 nd ns-interval** *milliseconds*

**no ipv6 nd ns-interval**

*milliseconds* - The interval between transmitting IPv6 neighbor solicitation messages. (Range: 1000-3600000)

### DEFAULT SETTING

1000 milliseconds is used for neighbor discovery operations
0 milliseconds is advertised in router advertisements

### COMMAND MODE

Interface Configuration (VLAN)

### COMMAND USAGE

- When a non-default value is configured, the specified interval is used both for router advertisements and by the router itself.
- This command specifies the interval between transmitting neighbor solicitation messages when resolving an address, or when probing the reachability of a neighbor. Therefore, avoid using very short intervals for normal IPv6 operations.

### EXAMPLE

The following sets the interval between sending neighbor solicitation messages to 30000 milliseconds:

```
Console(config)#interface vlan 1
Console(config)#ipv6 nd ns-interval 30000
Console(config)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::2E0:CFF:FE9C:CA10/64
Global unicast address(es):
  2001:DB8:2222:7272::/64, subnet is 2001:DB8:2222:7272::/64
  2009:DB9:2229::79, subnet is ::
Joined group address(es):
FF02::2
FF02::1:FF00:0
FF02::1:2
FF02::1:FF9C:CA10
FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 2.
ND retransmit interval is 30000 milliseconds
Console#
```

#### RELATED COMMANDS

show running-config (617)

## ipv6 nd reachable-time

This command configures the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred.

#### SYNTAX

**ipv6 nd reachable-time** *milliseconds*

**no ipv6 nd reachable-time**

*milliseconds* - The time that a node can be considered reachable after receiving confirmation of reachability.
(Range: 1000-3600000)

#### DEFAULT SETTING

30000 milliseconds is used for neighbor discovery operations
0 milliseconds is advertised in router advertisements

#### COMMAND MODE

Interface Configuration (VLAN)

#### COMMAND USAGE

- The time limit configured by this command allows the router to detect unavailable neighbors.
- This time limit is included in all router advertisements sent out through an interface, ensuring that nodes on the same link use the same time value.
- Setting the time limit to 0 means that the configured time is unspecified by this router.

**EXAMPLE**

The following sets the reachable time for a remote node to 1000 milliseconds:

```
Console(config)#interface vlan 1
Console(config)#pv6 nd reachable-time 1000
Console(config)#
```

## clear ipv6 neighbors

This command deletes all dynamic entries in the IPv6 neighbor discovery cache.

**COMMAND MODE**

Privileged Exec

**EXAMPLE**

The following deletes all dynamic entries in the IPv6 neighbor cache:

```
Console#clear ipv6 neighbors
Console#
```

## show ipv6 neighbors

This command displays information in the IPv6 neighbor discovery cache.

**SYNTAX**

**show ipv6 neighbors** [**vlan** *vlan-id* | *ipv6-address*]

*vlan-id* - VLAN ID (Range: 1-4093)

*ipv6-address* - The IPv6 address of a neighbor device. You can specify either a link-local or global unicast address formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

**DEFAULT SETTING**

All IPv6 neighbor discovery cache entries are displayed.

**COMMAND MODE**

Privileged Exec

**EXAMPLE**

The following shows all known IPv6 neighbors for this switch:

```
Console#show ipv6 neighbors
State: I1 - Incomplete, I2 - Invalid, R - Reachable, S - Stale, D - Delay,
      P1 - Probe, P2 - Permanent, U - Unknown
IPv6 Address                    Age      Link-layer Addr   State VLAN
FE80::2E0:CFF:FE9C:CA10            4        00-E0-0C-9C-CA-10     R    1
Console#
```

**Table 10: show ipv6 traffic** - display description

| Field | Description |
|---|---|
| IPv6 Address | IPv6 address of neighbor |
| Age | The time since the address was verified as reachable (in minutes). A static entry is indicated by the value “Permanent.” |
| Link-layer Addr | Physical layer MAC address. |
| State | The following states are used for dynamic entries:<br>I1 (Incomplete) - Address resolution is being carried out on the entry. A neighbor solicitation message has been sent to the multicast address of the target, but it has not yet returned a neighbor advertisement message.<br>I2 (Invalid) - An invalidated mapping. Setting the state to invalid dis-associates the interface identified with this entry from the indicated mapping (RFC 4293).<br>R (Reachable) - Positive confirmation was received within the last ReachableTime interval that the forward path to the neighbor was functioning. While in REACH state, the device takes no special action when sending packets.<br>S (Stale) - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. While in STALE state, the device takes no action until a packet is sent.<br>D (Delay) - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. A packet was sent within the last DELAY_FIRST_PROBE_TIME interval. If no reachability confirmation is received within this interval after entering the DELAY state, the switch will send a neighbor solicitation message and change the state to PROBE.<br>P1 (Probe) - A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer interval until confirmation of reachability is received.<br>U (Unknown) - Unknown state.<br><br>The following states are used for static entries:<br>I1 (Incomplete)-The interface for this entry is down.<br>R (Reachable) - The interface for this entry is up. Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache.<br>P2 (Permanent) - Indicates a static entry. |
| VLAN | VLAN interface from which the address was reached. |

### RELATED COMMANDS

show mac-address-table (855)

## IPV6 TO IPV4 TUNNELS

This switch supports connection between isolated IPv6 nodes over IPv4 networks using manually configured tunnels (RFC 2893), as well as the connection of isolated IPv6 domains over IPv4 clouds without explicit tunnel configuration (RFC 3056).

**Table 11: IPv6 to IPv4 Tunnelling Commands**

| Command | Function | Mode |
|---|---|---|
| interface tunnel | Configures a tunnel interface and enters tunnel configuration mode | GC |
| ipv6 address | Configures an IPv6 global unicast address, and enables IPv6 on an interface | IC (tunnel) |
| ipv6 address link-local | Configures an IPv6 link-local address for an interface and enables IPv6 on the interface | IC (tunnel) |
| ipv6 address eui-64 | Configures an IPv6 global unicast address for an interface using an EUI-64 interface ID in the low order 64 bits, and enables IPv6 on the interface | IC (tunnel) |

**Table 11: IPv6 to IPv4 Tunnelling Commands (Continued)**

| Command | Function | Mode |
|---|---|---|
| tunnel destination[1] | Configures the IPv4 address of a tunnel destination | IC (tunnel) |
| tunnel mode ipv6ip | Configures the tunnel mode to manual configuration or 6-to-4 automatic tunneling | IC (tunnel) |
| tunnel source vlan | Sets the VLAN to which a tunnel source is assigned | IC (tunnel) |
| tunnel ttl | Configures the TTL value in the IPv4 header of a packet used for tunneling IPv6 traffic | IC (tunnel) |
| show ipv6 tunnel | Displays the status and configuration settings for all IPv6 over IPv4 tunnels | PE |

1. The tunnel destination only applies to manually configured tunneling (RFC 2893).

### COMMAND USAGE

To create a manually configured or automatically configured tunnel, follow these steps:

1. Configure a VLAN with the vlan command.

2. Assign the ports which will use this VLAN for local services, and those which will form the entry point for the IPv6 over IPv4 tunnel (using the switchport allowed vlan command.

3. Assign an IPv4 address to the VLAN to serve as the source (or local end point) of the tunnel using the ip address command.

4. Create an IPv6 over IPv4 tunnel using the interface tunnel command.

5. Set the tunnel mode to “configured” for host-to-router or router-to-router connections, or “6to4” for router-to-host or host-to-host connections using the tunnel mode ipv6ip command.

6. For “configured” tunnel mode, specify the IPv4 address of the far end of the tunnel using the tunnel destination command.

7. Bind the tunnel to a VLAN with the tunnel source vlan command.

8. Assign an IPv6 global unicast address to the tunnel using the ipv6 address command.

9. Then check your configuration settings using the show ipv6 tunnel command, and the interface status of the tunnel using the show ip interface or show ip interface brief command.

## interface tunnel

This command configures an IPv6 to IPv4 tunnel interface and enters tunnel configuration mode. Use the **no** form with a tunnel number to remove a tunnel, or without a tunnel number to remove all tunnels.

### SYNTAX

**interface tunnel** *tunnel-number*

**no interface tunnel** [*tunnel-number*]

*tunnel-number* - Tunnel interface identifier. (Range: 1-16)

### DEFAULT SETTING

None

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- Although this command is labeled with the name “tunnel,” it allows configuration of either a manually configured IPv6 over IPv4 transport network based on RFC 2893, or of an automatic method of transporting IPv6 traffic over IPv4 clouds without explicit tunnels using RFC 3056.
- Configured IPv6 over IPv4 tunneling uses point-to-point tunnels by encapsulating IPv6 packets within IPv4 headers to carry them over IPv4 routing infrastructures.
- Transporting IPv6 over IPv4 clouds (based on RFC 3056) defines a method for assigning a unique IPv6 address prefix to any site that currently has at least one globally unique IPv4 address, and specifies an encapsulation mechanism for transmitting IPv6 packets using such a prefix over the global IPv4 network.

### EXAMPLE

```
Console(config)#interface tunnel 1
Console(config-if)#
```

## tunnel destination

This command sets the IPv4 address of a tunnel destination (or far end-point of a tunnel). Use the **no** form to remove the assigned IPv4 address.

### SYNTAX

**tunnel destination** *ip-address*

**no tunnel destination**

*ip-address* - IPv4 address of the device at the far end of the tunnel.

### DEFAULT SETTING

None

### COMMAND MODE

Interface Configuration (IPv6/v4 Tunnel)

### Command Usage

- This command is only applicable to the “configured” tunnel mode (see the tunnel mode ipv6ip command).

- When an IPv6 packet is transmitted over a tunnel, the tunnel end-point address configured by this command is used as the destination address for the encapsulating IPv4 header.

- The determination of which packets to tunnel is based on information in the routing table, which directs packets based on their destination address using the prefix mask and match technique.

- IPv6/IPv4 hosts that are connected to data links with no IPv6 routers may use a configured tunnel to reach an IPv6 router. This tunnel allows the host to communicate with the rest of the IPv6 Internet (i.e., nodes with IPv6-native addresses). If the IPv4 address of an IPv6/IPv4 router bordering the IPv6 backbone is known, this can be used as the tunnel end-point address. This tunnel can be configured into the routing table as an IPv6 “default route.” That is, all IPv6 destination addresses will match the route and could potentially traverse the tunnel. Since the “mask length” of such a default route is zero, it will be used only if there are no other routes with a longer mask that match the destination. Note that the default configured tunnel can also be used in conjunction with 6to4 automatic tunneling.

- The tunnel end-point address of a default tunnel could be the IPv4 address of one IPv6/IPv4 router at the border of the IPv6 backbone. Alternatively, the tunnel end point could be an IPv4 “anycast address.” Using this approach, multiple IPv6/IPv4 routers at the border advertise IPv4 reachability to the same IPv4 address. All of these routers accept packets to this address as their own, and will decapsulate IPv6 packets tunneled to this address. When an IPv6/IPv4 node sends an encapsulated packet to this address, it will be delivered to only one of the border routers, usually the closest one.

- Care must be taken when using a default tunnel to prevent different IPv4 fragments from arriving at different routers for reassembly. This can be prevented by either avoiding fragmentation of the encapsulated packets (by ensuring an IPv4 MTU of at least 1300 bytes is used) or by preventing frequent changes to IPv4 routing.

- Packets delivered to transport protocols on the decapsulating node should not be subject to ingress filtering. For bidirectionally configured tunnels this is done by verifying that the source address is the IPv4 address of the other end of the tunnel. For unidirectionally configured tunnels, the decapsulating node must be configured with a list of source IPv4 address prefixes that are acceptable. Such a list must default to not having any entries, i.e. the node has to be explicitly configured to forward decapsulated packets received over unidirectionally configured tunnels.

### Example

```
Console(config)#interface tunnel 2
Console(config-if)#tunnel destination 192.168.1.5
Console(config-if)#
```

## tunnel mode ipv6ip

This command sets the tunnel mode to manual configuration or 6-to-4 automatic tunneling. Use the **no** form to restore the default setting.

### SYNTAX

**tunnel mode ipv6ip** {**configured** | **6to4**}

**no tunnel mode ipv6ip**

**configured** - Configured IPv6 over IPv4 tunneling using point-to-point tunnels by encapsulating IPv6 packets within IPv4 headers to carry them over IPv4 routing infrastructures (based on RFC 2893).

**6to4** - Transports IPv6 over IPv4 clouds by assigning a unique IPv6 address prefix to any site that currently has at least one globally unique IPv4 address, and specifying an encapsulation mechanism for transmitting IPv6 packets using such a prefix over the global IPv4 network. (This method is based on RFC 3056.)

### DEFAULT SETTING

configured

### COMMAND MODE

Interface Configuration (IPv6/v4 Tunnel)

### COMMAND USAGE

- Configured tunneling of IPv6 over IPv4 based on RFC 2893 uses point-to-point tunnels made by encapsulating IPv6 packets within IPv4 headers to carry them over IPv4 routing infrastructures. These tunnels can be either unidirectional or bidirectional. Bidirectionally configured tunnels behave as virtual point-to-point links. When using configured tunnels, the IPv4 tunnel end-point address must be manually configured on the encapsulating node with the tunnel destination command.

  The 6to4 mechanism is typically implemented almost entirely in routers bordering between IPv4 and IPv6 domains.

  The tunnel end-point address of a 6to4 tunnel is dynamically determined by the tunnel source (local end-point node) via the IPv6 6to4 address of the packet sent from IPv6 6to4 hosts. The 6to4 end-point address is constructed using "2002:*Public IPv4 Address*::/48" as the IPv6 address prefix. This prefix can be used exactly like any other valid IPv6 prefix, e.g., for "Neighbor Discovery for IP Version 6 (IPv6)" defined in RFC 2461.

- IPv6/IPv4 hosts and routers can tunnel IPv6 datagrams over regions of IPv4 routing topology by encapsulating them within IPv4 packets. Tunneling can be used in a variety of ways, including the following:

  - Router-to-Router: IPv6/IPv4 routers interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves. In this case, the tunnel spans one segment of the end-to-end path that the IPv6 packet takes.
  - Host-to-Router: IPv6/IPv4 hosts can tunnel IPv6 packets to an intermediate IPv6/IPv4 router that is reachable via an IPv4 infrastructure. This type of tunnel spans the first segment of the packet's end-to-end path.

- Host-to-Host: IPv6/IPv4 hosts that are interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves. In this case, the tunnel spans the entire end-to-end path that the packet takes; and a host can be either a 6to4 node or native IPv6 host.
- Router-to-Host: IPv6/IPv4 routers can tunnel IPv6 packets to their final destination IPv6/IPv4 host. This tunnel spans only the last segment of the end-to-end path.

Tunneling techniques are classified according to the mechanism by which the encapsulating node determines the address of the node at the end of the tunnel. In the first two tunneling methods listed above – router-to-router and host-to-router – the IPv6 packet is being tunneled to a router. The end point of this type of tunnel is an intermediate router which must decapsulate the IPv6 packet and forward it on to its final destination. When tunneling to a router, the end point of the tunnel is different from the destination of the packet being tunneled. So the addresses in the IPv6 packet being tunneled can not provide the IPv4 address of the tunnel end point. Instead, the tunnel end-point address must be determined from information configured on the encapsulating node. In other words, “configured tunneling” must be used to explicitly identify the end point.

In the last two tunneling methods – host-to-host and router-to-host – the IPv6 packet is tunneled all the way to its final destination. In this case, the destination address of both the IPv6 packet and the encapsulating IPv4 header identify the same node. This fact can be exploited by encoding information in the IPv6 destination address that will allow the encapsulating node to determine the tunnel end point IPv4 address automatically. “6to4 automatic tunneling” employs this technique, using an special IPv6 address format with an embedded IPv4 address to allow tunneling nodes to automatically derive the tunnel end-point IPv4 address. This eliminates the need to explicitly configure the tunnel end-point address.

■ The two tunneling techniques – configured and automatic – differ primarily in how they determine the tunnel end-point address. Most of the underlying mechanisms are the same:

- The entry node of the tunnel (the encapsulating node) creates an encapsulating IPv4 header and transmits the encapsulated packet.
- The exit node of the tunnel (the decapsulating node) receives the encapsulated packet, reassembles the packet if needed, removes the IPv4 header, updates the IPv6 header, and processes the received IPv6 packet.

### EXAMPLE

```
Console(config)#interface tunnel 2
Console(config-if)#tunnel mode ipv6ip configured
Console(config-if)#
```

## tunnel source vlan

This command sets the VLAN to which a tunnel source (or local end-point of a tunnel) is assigned. Use the **no** form to detach the tunnel from the assigned VLAN.

#### SYNTAX

**tunnel source vlan** *vlan-id*

**no tunnel source vlan**

*vlan-id* - VLAN ID (Range: 1-4093)

#### DEFAULT SETTING

None

#### COMMAND MODE

Interface Configuration (IPv6/v4 Tunnel)

#### COMMAND USAGE

The VLAN assigned to a tunnel must be a L3 VLAN with an IPv4 address. Otherwise, an error message will be displayed on the console.

#### EXAMPLE

```
Console(config)#interface tunnel 2
Console(config-if)#tunnel source vlan 2
Console(config-if)#
```

### tunnel ttl

This command configures the TTL (Time to Live) value stored in the IPv4 header of a packet used for tunneling IPv6 traffic. Use the **no** form to restore the default value.

#### SYNTAX

**tunnel ttl** *ttl-value*

**no tunnel ttl**

*ttl-value* - The TTL value of the IPv4 encapsulating packet. (Range: 0-255, where zero means that the TTL value is taken from the Hop Limit set in the IP header of the encapsulated IPv6 packet)

#### DEFAULT SETTING

0

#### COMMAND MODE

Interface Configuration (IPv6/v4 Tunnel)

#### COMMAND USAGE

The command sets the hop limit for the IPv4 encapsulating packet. However, note that IPv6 over IPv4 tunnels are modeled as a “single-hop.” That is, the IPv6 hop limit is decremented by only one when an IPv6 packet traverses the tunnel. The single-hop model serves to hide the existence of a tunnel. The tunnel is opaque to users of the network, and is not detectable by network diagnostic tools such as traceroute.

### EXAMPLE

```
Console(config)#interface tunnel 2
Console(config-if)#tunnel ttl 5
Console(config-if)#
```

## show ipv6 tunnel

This command displays the status and configuration settings for all IPv6 over IPv4 tunnels.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show ipv6 tunnel

Tunnel:1
 Tunnel Current State                    : Up
 Tunnel Source Address                   : [VLAN1]192.168.0.3
 Tunnel Destination Address              : 192.168.0.2
 Time to Live                            : 255
 Tunnel Mode (Configured / 6-to-4 / ISATAP) : Configured

Console#
```

The following example shows the interface status of the configured tunnels.

```
Console#show ipv6 interface
Vlan 1 is up
IPv6 is stale.
Link-local address:
(None)
Global unicast address(es):
(None)
Joined group address(es):
FF02::1:2
FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 2.
ND retransmit interval is 1000 milliseconds

Tunnel 1 is up
IPv6 is stale.
Link-local address:
  FE80::C0A8:3/64
Global unicast address(es):
  2002:DB9:2222:7272::72/48, subnet is 2002:DB9:2222::/48
Joined group address(es):
FF02::1
IPv6 link MTU is 0 bytes
ND DAD is enabled, number of DAD attempts: 2.
ND retransmit interval is 1000 milliseconds

Console#show ipv6 interface brief
Interface      VLAN       IPv6       IPv6 Address
-------------- ---------- ---------- ----------------------------------------
VLAN 1         Up         Down       Unassigned
TUNNEL 1       Up         Down       2002:DB9:2222:7272::72/48
```

```
TUNNEL 1      Up      Down      FE80::C0A8:3

Console#
```

# 48 IP ROUTING COMMANDS

After network interfaces are configured for the switch, the paths used to send traffic between different interfaces must be set. If routing is enabled on the switch, traffic will automatically be forwarded between all of the local subnetworks. However, to forward traffic to devices on other subnetworks, either configure fixed paths with static routing commands, or enable a dynamic routing protocol that exchanges information with other routers on the network to automatically determine the best path to any subnetwork.

This section includes commands for both static and dynamic routing. These commands are used to connect between different local subnetworks or to connect the router to the enterprise network.

**Table 1: IP Routing Commands**

| Command Group | Function |
|---|---|
| Global Routing Configuration | Configures global parameters for static and dynamic routing, displays the routing table and statistics for protocols used to exchange routing information |
| Routing Information Protocol (RIP) | Configures global and interface specific parameters for RIP |
| Open Shortest Path First (OSPFv2) | Configures global and interface specific parameters for OSPFv2 |
| Open Shortest Path First (OSPFv3) | Configures global and interface specific parameters for OSPFv3 |

## GLOBAL ROUTING CONFIGURATION

**Table 2: Global Routing Configuration Commands**

| Command | Function | Mode |
|---|---|---|
| *IPv4 Commands* | | |
| ip route | Configures static routes | GC |
| maximum-paths | Sets the maximum number of paths allowed | GC |
| show ip route | Displays specified entries in the routing table | PE |
| show ip route database | Displays static or dynamically learned entries in the routing table | PE |
| show ip traffic | Displays statistics for IP, ICMP, UDP, TCP and ARP protocols | PE |
| *IPv6 Commands* | | |
| ipv6 route | Configures static routes | GC |
| show ipv6 route | Displays specified entries in the routing table | PE |

**ip route** This command configures static routes. Use the **no** form to remove static routes.

### SYNTAX

**ip route** *destination-ip netmask next-hop* [*distance*]

**no ip route** {*destination-ip netmask next-hop* | *}

*destination-ip* – IP address of the destination network, subnetwork, or host.

*netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.

*next-hop* – IP address of the next hop router used for this route.

*distance* – An administrative distance indicating that this route can be overridden by dynamic routing information if the distance of the dynamic route is less than that configured for the static route. Note that the default administrative distances used by the dynamic unicast routing protocols is 110 for OSPF and 120 for RIP.
(Range: 1-255, Default: 1)

* – Removes all static routing table entries.

### DEFAULT SETTING

No static routes are configured.

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- Up to 512 static routes can be configured.
- Up to eight equal-cost multipaths (ECMP) can be configured for static routing using the maximum-paths command.
- If an administrative distance is defined for a static route, and the same destination can be reached through a dynamic route at a lower administration distance, then the dynamic route will be used.
- If both static and dynamic paths have the same lowest cost, the first route stored in the routing table, either statically configured or dynamically learned via a routing protocol, will be used.
- Static routes are included in RIP and OSPF updates periodically sent by the router if this feature is enabled by the RIP or OSPF redistribute command (see page 1127 or page 1147, respectively).

### EXAMPLE

This example forwards all traffic for subnet 192.168.1.0 to the gateway router 192.168.5.254, using the default metric of 1.

```
Console(config)#ip route 192.168.1.0 255.255.255.0 192.168.5.254
Console(config)#
```

## maximum-paths

This command sets the maximum number of paths allowed. Use the no form to restore the default settings.

### SYNTAX

**maximum-paths** *path-count*

**no maximum-paths**

*path-count* - The maximum number of equal-cost paths to the same destination that can be installed in the routing table. (Range: 1-8)

### DEFAULT SETTING

Enabled, 4 paths

### COMMAND MODE

Global Configuration

### EXAMPLE

```
switch(config)#maximum-paths 8
switch(config)#
```

## show ip route

This command displays information in the Forwarding Information Base (FIB).

### SYNTAX

**show ip route** [**connected** | **ospf** | **rip** | **static** | **summary**]

**connected** – Displays all currently connected entries.

**ospf** – Displays external routes imported from the Open Shortest Path First (OSPF) protocol into this routing domain.

**rip** – Displays all entries learned through the Routing Information Protocol (RIP).

**static** – Displays all static entries.

**summary** – Displays a brief list of summary information about entries in the routing table, including the maximum number of entries supported, the number of connected routes, the total number of routes currently stored in the routing table, and the number of entries in the FIB.

### COMMAND MODE

Privileged Exec

### COMMAND USAGE

- The FIB contains information required to forward IP traffic. It contains the interface identifier and next hop information for each reachable destination network prefix based on the IP routing table. When routing or topology changes occur in the network, the routing table is updated, and those changes are immediately reflected in the FIB.

The FIB is distinct from the routing table (or, Routing Information Base), which holds all routing information received from routing peers. The forwarding information base contains unique paths only. It does not contain any secondary paths. A FIB entry consists of the minimum amount of information necessary to make a forwarding decision on a particular packet. The typical components within a forwarding information base entry are a network prefix, a router port identifier, and next hop information.

- This command only displays routes which are currently accessible for forwarding. The router must be able to directly reach the next hop, so the VLAN interface associated with any dynamic or static route entry must be up. Note that routes currently not accessible for forwarding, may still be displayed by using the show ip route database command.

#### Example

In the following example, note that the entry for RIP displays both the distance and metric for this route.

```
Console#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

R      10.1.1.0/24 [120/2] via 192.168.1.10, VLAN1, 00:00:14
C      127.0.0.0/8 is directly connected, lo
C      192.168.1.0/24 is directly connected, VLAN1
Console#
```

### show ip route database

This command displays entries in the Routing Information Base (RIB).

#### Command Mode

Privileged Exec

#### Command Usage

The RIB contains all available routes learned through dynamic routing protocols, directly attached networks, and any additionally configured routes such as static routes. The RIB contains the set of all available routes from which optimal entries are selected for use by the Forwarding Information Base (see Command Usage under the show ip route command).

#### Example

```
Console#show ip route database
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

C    *> 127.0.0.0/8 is directly connected, lo0
```

```
C    *> 192.168.1.0/24 is directly connected, VLAN1

Console#
```

## show ip traffic

This command displays statistics for IP, ICMP, UDP, TCP and ARP protocols.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show ip traffic
IP Statistics:
IP received
            4877 total received
                header errors
                unknown protocols
                address errors
                discards
            4763 delivers
                reassembly request datagrams
                reassembled succeeded
                reassembled failed
IP sent
                forwards datagrams
            5927 requests
                discards
                no routes
                generated fragments
                fragment succeeded
                fragment failed
ICMP Statistics:
ICMP received
                input
                errors
                destination unreachable messages
                time exceeded messages
                parameter problem message
                echo request messages
                echo reply messages
                redirect messages
                timestamp request messages
                timestamp reply messages
                source quench messages
                address mask request messages
                address mask reply messages
ICMP sent
                output
                errors
                destination unreachable messages
                time exceeded messages
                parameter problem message
                echo request messages
                echo reply messages
                redirect messages
                timestamp request messages
                timestamp reply messages
                source quench messages
                address mask request messages
                address mask reply messages
```

```
UDP Statistics:
            2 input
              no port errors
              other errors
              output
TCP Statistics:
          4698 input
              input errors
          5867 output

Console#
```

**ipv6 route** This command configures static IPv6 routes. Use the **no** form to remove static routes.

### Syntax

[**no**] **ipv6 route** *destination-ipv6-address*/*prefix-length*
{*gateway-address* [*distance*] |
*link-local-address***%***zone-id* [*distance*] |
**tunnel** *interface-number*}

*destination-ipv6-address* – The IPv6 address of a destination network, subnetwork, or host. This must be a full IPv6 address including the network prefix and host address bits.

*prefix-length* - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

*gateway-address* – IP address of the next hop router used for this route.

*link-local-address***%***zone-id* – a link-local address, including a zone-id indicating the VLAN identifier after the % delimiter.

*distance* – An administrative distance indicating that this route can be overridden by dynamic routing information if the distance of the dynamic route is less than that configured for the static route. Note that the default administrative distances used by the dynamic unicast routing protocols is 110 for OSPF and 120 for RIP. (Range: 1-255, Default: 1)

*interface-number* – The number of the outgoing tunnel interface used to reach the destination IPv6 address. (Range: 1-16)
See the interface tunnel command for more information.

### Default Setting
No static routes are configured.

### Command Mode
Global Configuration

### Command Usage
- Up to 1K static routes can be configured.

- Up to eight equal-cost multipaths (ECMP) can be configured for static routing using the maximum-paths command.

- If an administrative distance is defined for a static route, and the same destination can be reached through a dynamic route at a lower administration distance, then the dynamic route will be used.
- The default distance of 1 will take precedence over any other type of route, except for local routes.
- If both static and dynamic paths have the same lowest cost, the first route stored in the routing table, either statically configured or dynamically learned via a routing protocol, will be used.
- Static routes are included in RIP and OSPF updates periodically sent by the router if this feature is enabled by the OSPFv3 redistribute command.

### EXAMPLE

This example forwards all traffic for subnet 2001::/64 to the next hop router 2001:DB8:2222:7272::254, using the default metric of 1.

```
Console(config)#ipv6 route 2001::/64 2001:DB8:2222:7272::254
Console(config)#
```

### RELATED COMMANDS

show ip route summary (1115)

## show ipv6 route

This command displays information in the Forwarding Information Base (FIB).

### SYNTAX

**show ipv6 route ospf | rip | static | local | interface vlan** *vlan-id* | *ipv6-address*[/ *prefix-length*]]

**ospf** – Displays external routes imported from the Open Shortest Path First (OSPF) protocol into this routing domain.

**rip** – Displays all entries learned through the Routing Information Protocol (RIP).

**static** – Displays all static entries.

**local** – Displays all entries for destinations attached directly to this router.

**interface** – Displays all routes that be accessed through this interface.

*ipv6-address* - A full IPv6 address including the network prefix and host address bits.

*prefix-length* - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

### COMMAND MODE

Privileged Exec

### COMMAND USAGE

- The FIB contains information required to forward IP traffic. It contains the interface identifier and next hop information for each reachable destination network prefix based on the IP routing table. When routing or topology changes occur in the network, the routing table is updated, and those changes are immediately reflected in the FIB.

  The FIB is distinct from the routing table (or, Routing Information Base), which holds all routing information received from routing peers. The forwarding information base contains unique paths only. It does not contain any secondary paths. A FIB entry consists of the minimum amount of information necessary to make a forwarding decision on a particular packet. The typical components within a forwarding information base entry are a network prefix, a router port identifier, and next hop information.

- This command only displays routes which are currently accessible for forwarding. The router must be able to directly reach the next hop, so the VLAN interface associated with any dynamic or static route entry must be up.

### EXAMPLE

In the following example, note that the last entry displays both the distance and metric for this route.

```
Console#show ipv6 route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
C    ::1/128, lo0
?    FE80::/64, VLAN1 inactive
C    FE80::/64, VLAN1
?    FF00::/8, VLAN1 inactive
O IA 3FFF:1::/32 [110/3]
      via FE80::204:FF:FE05:6, VLAN1

Console#
```

## ROUTING INFORMATION PROTOCOL (RIP)

**Table 3: Routing Information Protocol Commands**

| Command | Function | Mode |
|---|---|---|
| router rip | Enables the RIP routing protocol | GC |
| default-information originate | Generates a default external route into an autonomous system | RC |
| default-metric | Sets the default metric assigned to external routes imported from other protocols | RC |
| distance | Defines an administrative distance for external routes learned from other routing protocols | RC |
| maximum-prefix | Sets the maximum number of RIP routes allowed | RC |

**Table 3: Routing Information Protocol Commands (Continued)**

| Command | Function | Mode |
|---|---|---|
| neighbor | Defines a neighboring router with which to exchange information | RC |
| network | Specifies the network interfaces that are to use RIP routing | RC |
| passive-interface | Stops RIP from sending routing updates on the specified interface | RC |
| redistribute | Redistribute routes from one routing domain to another | RC |
| timers basic | Sets basic timers, including update, timeout, garbage collection | RC |
| version | Specifies the RIP version to use on all network interfaces (if not already specified with a receive version or send version command) | RC |
| ip rip authentication mode | Specifies the type of authentication used for RIP2 packets | IC |
| ip rip authentication string | Enables authentication for RIP2 packets and specifies keys | IC |
| ip rip receive version | Sets the RIP receive version to use on a network interface | IC |
| ip rip receive-packet | Configures the interface to receive of RIP packets | IC |
| ip rip send version | Sets the RIP send version to use on a network interface | IC |
| ip rip send-packet | Configures the interface to send RIP packets | IC |
| ip rip split-horizon | Enables split-horizon or poison-reverse loop prevention | IC |
| clear ip rip route | Clears specified data from the RIP routing table | PE |
| show ip protocols rip | Displays RIP process parameters | PE |
| show ip rip | Displays information about RIP routes and configuration settings | PE |

## router rip

This command enables Routing Information Protocol (RIP) routing for all IP interfaces on the router. Use the **no** form to disable it.

### SYNTAX

[**no**] **router rip**

### COMMAND MODE

Global Configuration

### DEFAULT SETTING

Disabled

### COMMAND USAGE

- RIP is used to specify how routers exchange routing table information.
- This command is also used to enter router configuration mode.

#### Example

```
Console(config)#router rip
Console(config-router)#
```

#### Related Commands

network (1125)

### default-information originate

This command generates a default external route into the local RIP autonomous system. Use the **no** form to disable this feature.

#### Syntax

[**no**] **default-information originate**

#### Default Setting

Disabled

#### Command Mode

Router Configuration

#### Command Usage

This command sets a default route for every Layer 3 interface where RIP is enabled. The response packet to external queries marks each active RIP interface as a default router with the IP address 0.0.0.0.

#### Example

```
Console(config-router)#default-information originate
Console(config-router)#
```

#### Related Commands

ip route (1114)
redistribute (1127)

### default-metric

This command sets the default metric assigned to external routes imported from other protocols. Use the **no** form to restore the default value.

#### Syntax

**default-metric** *metric-value*

**no default-metric**

*metric-value* – Metric assigned to external routes. (Range: 1-15)

#### Default Setting

1

#### COMMAND MODE
Router Configuration

#### COMMAND USAGE
- This command does not override the metric value set by the redistribute command. When a metric value has not been configured by the redistribute command, the **default-metric** command sets the metric value to be used for all imported external routes.

- The default metric must be used to resolve the problem of redistributing external routes with incompatible metrics.

- It is advisable to use a low metric when redistributing routes from another protocol into RIP. Using a high metric limits the usefulness of external routes redistributed into RIP. For example, if a metric of 10 is defined for redistributed routes, these routes can only be advertised to routers up to 5 hops away, at which point the metric exceeds the maximum hop count of 15. By defining a low metric of 1, traffic can follow a imported route the maximum number of hops allowed within a RIP domain. However, note that using a low metric can increase the possibility of routing loops For example, this can occur if there are multiple redistribution points and the router learns about the same external network with a better metric from a redistribution point other than that derived from the original source.

#### EXAMPLE
This example sets the default metric to 5.

```
Console(config-router)#default-metric 5
Console(config-router)#
```

#### RELATED COMMANDS
redistribute (1127)

### distance
This command defines an administrative distance for external routes learned from other routing protocols. Use the **no** form to restore the default setting.

#### SYNTAX
[**no**] **distance** *distance network-address netmask* [*acl-name*]

*distance* - Administrative distance for external routes. External routes are routes for which the best path is learned from a neighbor external to the local RIP autonomous system. Routes with a distance of 255 are not installed in the routing table.
(Range: 1-255)

*network-address* - IP address of a route entry.

*netmask* - Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

*acl-name* - Name of the access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs. (Range: 1-16 characters)

**DEFAULT SETTING**
None

**COMMAND MODE**
Router Configuration

**COMMAND USAGE**

- Administrative distance is used by the routers to select the preferred path when there are two or more different routes to the same destination from two different routing protocols. A smaller administrative distance indicates a more reliable protocol.

- An access list can be used to filter networks according to the IP address of the router supplying the routing information. For example, to filter out unreliable routing information from routers not under your administrative control.

- The administrative distance is applied to all routes learned for the specified network.

**EXAMPLE**

```
Console(config-router)#distance 2 192.168.3.0 255.255.255.0
Console(config-router)#
```

## maximum-prefix

This command sets the maximum number of RIP routes allowed by the system. Use the **no** form to restore the default setting.

**SYNTAX**

**maximum-prefix** *maximum-routes*

**no maximum-prefix**

*maximum-routes* - The maximum number of RIP routes which can be installed in the routing table. (Range: 1-7168)

**DEFAULT SETTING**
1024

**COMMAND MODE**
Router Configuration

**COMMAND USAGE**
All the learned RIP routes may not be copied to the hardware tables in ASIC for fast data forwarding because of hardware resource limitations.

**EXAMPLE**

```
Console(config-router)#maximum-prefix 1024
Console(config-router)#
```

## neighbor

This command defines a neighboring router with which this router will exchange routing information. Use the **no** form to remove an entry.

### SYNTAX

[**no**] **neighbor** *ip-address*

*ip-address* - IP address of a neighboring router.

### DEFAULT SETTING

No neighbors are defined.

### COMMAND MODE

Router Configuration

### COMMAND USAGE

- This command can be used to configure a static neighbor (specifically for point-to-point links) with which this router will exchange routing information, rather than relying on broadcast or multicast messages generated by the RIP protocol.
- Use this command in conjunction with the passive-interface command to control the routing updates sent to specific neighbors.

### EXAMPLE

```
Console(config-router)#neighbor 10.2.0.254
Console(config-router)#
```

### RELATED COMMANDS

passive-interface (1126)

## network

This command specifies the network interfaces that will be included in the RIP routing process. Use the **no** form to remove an entry.

### SYNTAX

[**no**] **network** {*ip-address netmask* | **vlan** *vlan-id*}

*ip-address* – IP address of a network directly connected to this router.

*netmask* - Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

*vlan-id* - VLAN ID. (Range: 1-4093)

### DEFAULT SETTING

No networks are specified.

### COMMAND MODE

Router Configuration

#### COMMAND USAGE
RIP only sends and receives updates on interfaces specified by this command. If a network is not specified, the interfaces in that network will not be advertised in any RIP updates.

#### EXAMPLE
This example includes network interface 10.1.0.0 in the RIP routing process.

```
Console(config-router)#network 10.1.0.0
Console(config-router)#
```

#### RELATED COMMANDS
router rip (1121)

### passive-interface

This command stops RIP from sending routing updates on the specified interface. Use the **no** form to disable this feature.

#### SYNTAX
[**no**] **passive-interface vlan** *vlan-id*

*vlan-id* - VLAN ID. (Range: 1-4093)

#### DEFAULT SETTING
Disabled

#### COMMAND MODE
Router Configuration

#### COMMAND USAGE
- If this command is used to stop sending routing updates on an interface, the attached subnet will still continue to be advertised to other interfaces, and updates from other routers on that interface will continue to be received and processed.
- Use this command in conjunction with the neighbor command to control the routing updates sent to specific neighbors.

#### EXAMPLE

```
Console(config-router)#passive-interface vlan1
Console(config-router)#
```

#### RELATED COMMANDS
neighbor (1125)

## redistribute

This command imports external routing information from other routing domains (that is, directly connected routes, protocols, or static routes) into the autonomous system. Use the **no** form to disable this feature.

### SYNTAX

[**no**] **redistribute** (**connected** | **ospf** | **static**} [**metric** *metric-value*]

**connected** - Imports routes that are established automatically just by enabling IP on an interface.

**ospf** - External routes will be imported from the Open Shortest Path First (OSPF) protocol into this routing domain.

**static** - Static routes will be imported into this routing domain.

*metric-value* - Metric value assigned to all external routes for the specified protocol. (Range: 1-16)

### DEFAULT SETTING

redistribution - none
metric-value - set by the default-metric command

### COMMAND MODE

Router Configuration

### COMMAND USAGE

- When a metric value has not been configured by the **redistribute** command, the default-metric command sets the metric value to be used for all imported external routes.
- A route metric must be used to resolve the problem of redistributing external routes with incompatible metrics.
- It is advisable to use a low metric when redistributing routes from another protocol into RIP. Using a high metric limits the usefulness of external routes redistributed into RIP. For example, if a metric of 10 is defined for redistributed routes, these routes can only be advertised to routers up to 5 hops away, at which point the metric exceeds the maximum hop count of 15. By defining a low metric of 1, traffic can follow a imported route the maximum number of hops allowed within a RIP domain. However, using a low metric can increase the possibility of routing loops For example, this can occur if there are multiple redistribution points and the router learns about the same external network with a better metric from a redistribution point other than that derived from the original source.

### EXAMPLE

This example redistributes routes learned from OSPF and sets the metric for all external routes imported from OSPF to a value of 3.

```
Console(config-router)#redistribute ospf metric 3
Console(config-router)#
```

This example redistributes static routes and sets the metric for all of these routes to a value of 3.

```
Console(config-router)#redistribute static metric 3
Console(config-router)#
```

### RELATED COMMANDS

default-metric (1122)

## timers basic

This command configures the RIP update timer, timeout timer, and garbage- collection timer. Use the **no** form to restore the defaults.

### SYNTAX

**timers basic** *update timeout garbage*

**no timers basic**

*update* – Sets the update timer to the specified value. (Range: 5-2147483647 seconds)

*timeout* – Sets the timeout timer to the specified value. (Range: 90-360 seconds)

*garbage* – Sets the garbage collection timer to the specified value. (Range: 60-240 seconds)

### DEFAULT SETTING

Update: 30 seconds
Timeout: 180 seconds
Garbage collection: 120 seconds

### COMMAND MODE

Router Configuration

### COMMAND USAGE

- The *update* timer sets the rate at which updates are sent. This is the fundamental timer used to control all basic RIP processes.

- The *timeout* timer is the time after which there have been no update messages that a route is declared dead. The route is marked inaccessible (i.e., the metric set to infinite) and advertised as unreachable. However, packets are still forwarded on this route.

- After the *timeout* interval expires, the router waits for an interval specified by the *garbage-collection* timer before removing this entry from the routing table. This timer allows neighbors to become aware of an invalid route prior to it being purged by this device.

- Setting the update timer to a short interval can cause the router to spend an excessive amount of time processing updates.

- These timers must be set to the same values for all routers in the network.

#### EXAMPLE

This example sets the update timer to 40 seconds. The timeout timer is subsequently set to 240 seconds, and the garbage-collection timer to 160 seconds.

```
Console(config-router)#timers basic 15
Console(config-router)#
```

### version

This command specifies a RIP version used globally by the router. Use the **no** form to restore the default value.

#### SYNTAX

**version** {**1** | **2**}

**no version**

**1** - RIP Version 1

**2** - RIP Version 2

#### DEFAULT SETTING

Receive: Accepts RIPv1 or RIPv2 packets
Send: Route information is broadcast to other routers with RIPv2.

#### COMMAND MODE

Router Configuration

#### COMMAND USAGE

- When this command is used to specify a global RIP version, any VLAN interface not previously set by the ip rip receive version or ip rip send version command will use the global RIP version setting.

- When the **no** form of this command is used to restore the default value, any VLAN interface not previously set by the ip rip receive version or ip rip send version command will be set to the default send or receive version.

- Any configured interface settings take precedence over the global settings.

#### EXAMPLE

This example sets the global version for RIP to send and receive version 2 packets.

```
Console(config-router)#version 2
Console(config-router)#
```

#### RELATED COMMANDS

ip rip receive version (1131)
ip rip send version (1133)

## ip rip authentication mode

This command specifies the type of authentication that can be used for RIPv2 packets. Use the **no** form to restore the default value.

### Syntax

**ip rip authentication mode** {**md5** | **text**}

**no ip rip authentication mode**

**md5** - Message Digest 5 (MD5) authentication

**text** - Indicates that a simple password will be used.

### Default Setting

Text authentication

### Command Mode

Interface Configuration (VLAN)

### Command Usage

- The password to be used for authentication is specified in the ip rip authentication string command.
- This command requires the interface to exchange routing information with other routers based on an authorized password. (Note that this command only applies to RIPv2.)
- For authentication to function properly, both the sending and receiving interface must be configured with the same password or authentication key.
- MD5 is a one-way hash algorithm is that takes the authentication key and produces a 128 bit message digest or “fingerprint.” This makes it computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest.

### Example

This example sets the authentication mode to plain text.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip authentication mode text
Console(config-if)#
```

### Related Commands

ip rip authentication string (1130)

## ip rip authentication string

This command specifies an authentication key for RIPv2 packets. Use the **no** form to delete the authentication key.

### Syntax

**ip rip authentication string** *key-string*

**no ip rip authentication string**

*key-string* - A password used for authentication.
(Range: 1-16 characters, case sensitive)

### DEFAULT SETTING
No authentication key

### COMMAND MODE
Interface Configuration (VLAN)

### COMMAND USAGE
- This command can be used to restrict the interfaces that can exchange RIPv2 routing information. (Note that this command does not apply to RIPv1.)

- For authentication to function properly, both the sending and receiving interface must be configured with the same password, and authentication enabled by the ip rip authentication mode command.

### EXAMPLE
This example sets an authentication password of “small” to verify incoming routing messages and to tag outgoing routing messages.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip authentication string small
Console(config-if)#
```

### RELATED COMMANDS
ip rip authentication mode (1130)

## ip rip receive version

This command specifies a RIP version to receive on an interface. Use the **no** form to restore the default value.

### SYNTAX

**ip rip receive version** {**1** | **2**}

**no ip rip receive version**

**1** - Accepts only RIPv1 packets.

**2** - Accepts only RIPv2 packets.

### DEFAULT SETTING
RIPv1 or RIPv2 packets

### COMMAND MODE
Interface Configuration (VLAN)

### COMMAND USAGE
- Use this command to override the global setting specified by the RIP version command.

■You can specify the receive version based on these options:

- Use version 1 or version 2 if all routers in the local network are based on RIPv1 or RIPv2, respectively.
- Use the default of version 1 or 2 if some routers in the local network are using RIPv2, but there are still some older routers using RIPv1.

**EXAMPLE**
This example sets the interface version for VLAN 1 to receive RIPv1 packets.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip receive version 1
Console(config-if)#
```

**RELATED COMMANDS**
version (1129)

## ip rip receive-packet

This command configures the interface to receive RIP packets. Use the **no** form to disable this feature.

**SYNTAX**

[**no**] **ip rip receive-packet**

**DEFAULT SETTING**
Enabled

**COMMAND MODE**
Interface Configuration (VLAN)

**DEFAULT SETTING**
Enabled

**COMMAND USAGE**
Use the **no** form of this command if it is not required to add any dynamic entries to the routing table for an interface. For example, when only static routes are to be allowed for a specific interface.

**EXAMPLE**

```
Console(config)#interface vlan 1
Console(config-if)#ip rip receive-packet
Console(config-if)#
```

**RELATED COMMANDS**
ip rip send-packet (1133)

## ip rip send version

This command specifies a RIP version to send on an interface. Use the **no** form to restore the default value.

### SYNTAX

**ip rip send version** {**1** | **2** | **1-compatible**}

**no ip rip send version**

**1** - Sends only RIPv1 packets.

**2** - Sends only RIPv2 packets.

**1-compatible** - Route information is broadcast to other routers with RIPv2.

### DEFAULT SETTING

1-compatible (Route information is broadcast to other routers with RIPv2)

### COMMAND MODE

Interface Configuration (VLAN)

### COMMAND USAGE

- Use this command to override the global setting specified by the RIP version command.
- You can specify the send version based on these options:
  - Use version 1 or version 2 if all routers in the local network are based on RIPv1 or RIPv2, respectively.
  - Use "1-compatible" to propagate route information by broadcasting to other routers on the network using RIPv2, instead of multicasting as normally required by RIPv2. (Using this mode allows older RIPv2 routers which only receive RIP broadcast messages to receive all of the information provided by RIPv2, including subnet mask, next hop and authentication information.)

### EXAMPLE

This example sets the interface version for VLAN 1 to send RIPv1 packets.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip send version 1
Console(config-if)#
```

### RELATED COMMANDS

version (1129)

## ip rip send-packet

This command configures the interface to send RIP packets. Use the **no** form to disable this feature.

[**no**] **ip rip send-packet**

#### DEFAULT SETTING
Enabled

#### COMMAND MODE
Interface Configuration (VLAN)

#### DEFAULT SETTING
Enabled

#### COMMAND USAGE
The **no** form of this command allows the router to passively monitor route information advertised by other routers attached to the network, without transmitting any RIP updates.

#### EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip rip send-packet
Console(config-if)#
```

#### RELATED COMMANDS
ip rip receive-packet (1132)

### ip rip split-horizon

This command enables split-horizon or poison-reverse (a variation) on an interface. Use the **no** form to disable this function.

#### SYNTAX

**ip rip split-horizon** [**poisoned**]

**no rip ip split-horizon**

**poisoned** - Enables poison-reverse on the current interface.

#### COMMAND MODE
Interface Configuration (VLAN)

#### DEFAULT SETTING
split-horizon poisoned

#### COMMAND USAGE
- Split horizon never propagates routes back to an interface from which they have been acquired.
- Poison reverse propagates routes back to an interface port from which they have been acquired, but sets the distance-vector metrics to infinity. (This provides faster convergence.)
- If split-horizon is disabled with the **no rip ip split-horizon** command, and a loop occurs, the hop count for a route may be gradually incremented to infinity (that is, 16) before the route is deemed unreachable.

#### EXAMPLE

This example propagates routes back to the source using poison-reverse.

```
Console(config)#interface vlan 1
Console(config-if)#ip split-horizon poison-reverse
Console(config-if)#
```

### clear ip rip route

This command clears specified data from the RIP routing table.

#### SYNTAX

**clear ip rip route** {*ip-address netmask* **| all | connected | ospf | rip | static**}

*ip-address* - IP address of a route entry.

*netmask* - Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

**all** - Deletes all entries from the routing table.

**connected** - Deletes all currently connected entries.

**ospf** - Deletes all entries learned through the Open Shortest Path First routing protocol.

**rip** - Deletes all entries learned through the Routing Information Protocol.

**static** - Deletes all static entries.

#### DEFAULT SETTING

None

#### COMMAND MODE

Privileged Exec

#### COMMAND USAGE

Using this command with the “all” parameter clears the RIP table of all routes. To avoid deleting the entire RIP network, use the redistribute connected command to make the RIP network a connected route. To delete the RIP routes learned from neighbors and also keep the RIP network intact, use the “rip” parameter with this command (**clear ip rip route rip**).

#### EXAMPLE

This example clears one specific route.

```
Console#clear ip rip route 192.168.1.0 255.255.255.0
Console#
```

## show ip protocols rip

This command displays RIP process parameters.

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show ip protocols rip
Routing Protocol is "rip"
 Sending updates every 30 seconds with +/-5 seconds
 Timeout after 180 seconds, garbage collect after 120 seconds
 Outgoing update filter list for all interface is not set
 Incoming update filter list for all interface is not set
 Default redistribution metric is 1
 Redistributing:
 Default version control: send version by interface set,receive version by interface set
  Interface  Send        Recv
  VLAN1      1-compatible 1 2
 Routing for Networks:
  10.0.0.0/24
 Routing Information Sources:
  Gateway        Distance  Last Update  Bad Packets  Bad Routes
  10.0.0.2          120    00:00:13        0           0
 The maximum number of RIP routes allowed: 7872
 Distance: Default is 120
Console#
```

## show ip rip

This command displays information about RIP routes and configuration settings. Use this command without any keywords to display all RIP routes.

### SYNTAX

**show ip rip [interface [vlan** *vlan-id*]]

**interface** - Shows RIP configuration settings for all interfaces or for a specified interface.

*vlan-id* - VLAN ID. (Range: 1-4093)

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static,
       C - Connected, S - Static, O - OSPF

   Network          Next Hop       Metric From          Interface Time
Rc 192.168.0.0/24                  1                    VLAN1    01:57
Console#show ip rip interface vlan 1
Interface: vlan1
 Routing Protocol: RIP
  Receive RIPv1 and RIPv2 packets
  Send RIPv1 Compatible
  Passive interface: Disabled
  Authentication mode: (None)
```

```
    Authentication string: (None)
    Split horizon: Enabled with Poisoned Reverse
    IP interface address: 192.168.0.2/24
Console#
```

# Open Shortest Path First (OSPFv2)

**Table 4: Open Shortest Path First Commands**

| Command | Function | Mode |
|---|---|---|
| *General Configuration* | | |
| router ospf | Enables or disables OSPFv2 | GC |
| compatible rfc1583 | Calculates summary route costs using RFC 1583 (early OSPFv2) | RC |
| default-information originate | Generates a default external route into an autonomous system | RC |
| router-id | Sets the router ID for this device | RC |
| timers spf | Configures the delay after a topology change and the hold time between consecutive SPF calculations | RC |
| clear ip ospf process | Clears and restarts the OSPF routing process | PE |
| *Route Metrics and Summaries* | | |
| area default-cost | Sets the cost for a default summary route sent into a stub or NSSA | RC |
| area range | Summarizes routes advertised by an ABR | RC |
| auto-cost reference-bandwidth | Calculates default metrics for an interface based on bandwidth | RC |
| default-metric | Sets the default metric for external routes imported from other protocols | RC |
| redistribute | Redistribute routes from one routing domain to another | RC |
| summary-address | Summarizes routes advertised by an ASBR | RC |
| *Area Configuration* | | |
| area nssa | Defines a not-so-stubby that can import external routes | RC |
| area stub | Defines a stubby area that cannot send or receive LSAs | RC |
| area virtual-link | Defines a virtual link from an area border routers to the backbone | RC |
| network area | Assigns specified interface to an area | RC |
| *Interface Configuration* | | |
| ip ospf authentication | Specifies the authentication type for an interface | IC |
| ip ospf authentication-key | Assigns a simple password to be used by neighboring routers | IC |
| ip ospf cost | Specifies the cost of sending a packet on an interface | IC |
| ip ospf dead-interval | Sets the interval at which hello packets are not seen before neighbors declare the router down | IC |
| ip ospf hello-interval | Specifies the interval between sending hello packets | IC |
| ip ospf message-digest-key | Enables MD5 authentication and sets the key for an interface | IC |
| ip ospf priority | Sets the router priority used to determine the designated router | IC |
| ip ospf retransmit-interval | Specifies the time between resending a link-state advertisement | IC |
| ip ospf transmit-delay | Estimates time to send a link-state update packet over an interface | IC |

**Table 4: Open Shortest Path First Commands (Continued)**

| Command | Function | Mode |
|---|---|---|
| passive-interface | Suppresses OSPF routing traffic on the specified interface | RC |
| *Display Information* | | |
| show ip ospf | Displays general information about the routing processes | PE |
| show ip ospf border-routers | Displays routing table entries for Area Border Routers (ABR) and Autonomous System Boundary Routers (ASBR) | PE |
| show ip ospf database | Shows information about different LSAs in the database | PE |
| show ip ospf interface | Displays interface information | PE |
| show ip ospf neighbor | Displays neighbor information | PE |
| show ip ospf route | Displays the OSPF routing table | PE |
| show ip ospf virtual-links | Displays parameters and the adjacency state of virtual links | PE |
| show ip protocols ospf | Displays OSPF process parameters | PE |

## router ospf

This command enables Open Shortest Path First (OSPFv2) routing for all IP interfaces on the router and enters router configuration mode. Use the **no** form to disable OSPF for all processes or for a specified process.

### SYNTAX

[**no**] **router ospf** [*process-id*]

*process-id* - Process ID must be entered when configuring multiple routing instances. (Range: 1-65535; Default: 1)

### COMMAND MODE

Global Configuration

### DEFAULT SETTING

No routing process is defined.

### COMMAND USAGE

- OSPF is used to specify how routers exchange routing table information.
- This command is also used to enter router configuration mode.
- If the process ID is not defined, the default is instance 1.

### EXAMPLE

```
Console(config)#router ospf
Console(config-router)#
```

### RELATED COMMANDS

network area (1153)

## compatible rfc1583

This command calculates summary route costs using RFC 1583 (early OSPFv2). Use the **no** form to calculate costs using RFC 2328 (OSPFv2).

### SYNTAX

[**no**] **compatible rfc1583**

### COMMAND MODE

Router Configuration

### DEFAULT SETTING

RFC 1583 compatible

### COMMAND USAGE

- When RFC 1583 compatibility is enabled, only cost is used when choosing among multiple AS-external LSAs advertising the same destination. When disabled, preference is based on type of path (where type 1 external paths are preferred over type 2 external paths, using cost only to break ties (RFC 2328).

- All routers in an OSPF routing domain should use the same RFC for calculating summary routes.

- If there are any OSPF routers in an area exchanging summary information (specifically, ABRs) which have not been upgraded to OSPFv2, this command should be used on the newly upgraded OSPFv2 routers to ensure compatibility with routers still running older OSPFv2 code. Once all systems have been upgraded to newer OSPFv2 code, use the no form of this command to restore compatibility for all systems with RFC 2328.

### EXAMPLE

```
Console(config-router)#compatible rfc1583
Console(config-router)#
```

## default-information originate

This command generates a default external route into an autonomous system. Use the **no** form to disable this feature.

### SYNTAX

**default-information originate** [**always**] [**metric** *interface-metric*] [**metric-type** *metric-type*]

**no default-information originate** [**always** | **metric** | **metric-type**]

**always** - Always advertise itself as a default external route for the local AS regardless of whether the router has a default route. (See ?$paratext>? on page 1114.)

*interface-metric* - Metric assigned to the default route. (Range: 0-16777214)

*metric-type* - External link type used to advertise the default route. (Options: Type 1, Type 2)

### COMMAND MODE
Router Configuration

### DEFAULT SETTING
Disabled
Metric: 20
Metric Type: 2

### COMMAND USAGE
- If the **always** parameter is not selected, the router can only advertise a default external route into the AS if it has been configured to import external routes through other routing protocols or static routing, and such a route is known. (See the redistribute command.)

- The metric for the default external route is used to calculate the path cost for traffic passed from other routers within the AS out through the ASBR.

- When you use this command to redistribute routes into a routing domain (i.e., an Autonomous System, this router automatically becomes an Autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a default route into the routing domain.

  - If you use the **always** keyword, the router will advertise itself as a default external route into the AS, even if a default external route does not actually exist. To define a default route, use the ip route command.

  - If you do *not* use the **always** keyword, the router can only advertise a default external route into the AS if the redistribute command is used to import external routes via RIP or static routing, and such a route is known.

- Type 1 route advertisements add the internal cost to the external route metric. Type 2 routes do not add the internal cost metric. When comparing Type 2 routes, the internal cost is only used as a tie-breaker if several Type 2 routes have the same cost.

- This command should not be used to generate a default route for a stub or NSSA. To generate a default route for these area types, use the area stub or area nssa commands.

### EXAMPLE
This example assigns a metric of 20 to the default external route advertised into an autonomous system, sending it as a Type 2 external metric.

```
Console(config-router)#default-information originate metric 20 metric-type 2
Console(config-router)#
```

### RELATED COMMANDS
ip route (1114)
redistribute (1184)

## router-id

This command assigns a unique router ID for this device within the autonomous system for the current OSPF process. Use the **no** form to use the default router identification method (i.e., the highest interface address).

### Syntax

**router-id** *ip-address*

**no router-id**

*ip-address* - Router ID formatted as an IPv4 address.

### Command Mode

Router Configuration

### Default Setting

Highest interface address

### Command Usage

- This command sets the router ID for the OSPF process specified in the router ospf command.
- The router ID must be unique for every router in the autonomous system. Using the default setting based on the highest interface address ensures that each router ID is unique. (Note that the router ID can also be set to 0.0.0.0 or 255.255.255.255).
- If this router already has registered neighbors, the new router ID will be used when the router is rebooted, or manually restarted by entering the **no router ospf** followed by the **router ospf** command.
- If the priority values of the routers bidding to be the designated router or backup designated router for an area are equal, the router with the highest ID is elected.

### Example

```
Console(config-router)#router-id 10.1.1.1
Console(config-router)#
```

### Related Commands

router ospf (1139)

## timers spf

This command configures the delay after receiving a topology change and starting the shortest path first (SPF) calculation, and the hold time between making two consecutive SPF calculations. Use the **no** form to restore the default values.

### Syntax

**timers spf** *spf-delay spf-holdtime*

**no timers spf**

*spf-delay* - The delay after receiving a topology change notification and starting the SPF calculation. (Range: 0-2147483647 seconds) *spf-holdtime* - Minimum time between two consecutive SPF calculations. (Range: 0-2147483647 seconds)

#### COMMAND MODE
Router Configuration

#### DEFAULT SETTING
SPF delay: 5 seconds
SPF holdtime: 10 seconds

#### COMMAND USAGE
- Setting the SPF holdtime to 0 means that there is no delay between consecutive calculations.
- Using a low value allows the router to switch to a new path faster, but uses more CPU processing time.

#### EXAMPLE

```
Console(config-router)#timers spf 20
Console(config-router)#
```

### clear ip ospf process

This command clears and restarts the OSPF routing process. Specify the process ID to clear a particular OSPF process. When no process ID is specified, this command clears all running OSPF processes.

#### SYNTAX

**clear ip ospf** [*process-id*] **process**

*process-id* - Specifies the routing process ID. (Range: 1-65535)

#### DEFAULT SETTING
Clears all routing processes.

#### COMMAND MODE
Privileged Exec

#### EXAMPLE

```
Console#clear ip ospf process
Console#
```

## area default-cost

This command specifies a cost for the default summary route sent into a stub or NSSA from an Area Border Router (ABR). Use the **no** form to remove the assigned default cost.

### SYNTAX

**area** *area-id* **default-cost** *cost*

**no area** *area-id* **default-cost**

*area-id* - Identifies the stub or NSSA. (The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.)

*cost* - Cost for the default summary route sent to a stub or NSSA. (Range: 0-16777215)

### COMMAND MODE

Router Configuration

### DEFAULT SETTING

Default cost: 1

### COMMAND USAGE

- If the default cost is set to "0," the router will not advertise a default route into the attached stub or NSSA.

### EXAMPLE

```
Console(config-router)#area 10.3.9.0 default-cost 10
Console(config-router)#
```

### RELATED COMMANDS

area stub (1150)
area nssa (1149)

## area range

This command summarizes the routes advertised by an Area Border Router (ABR). Use the **no** form to disable this function.

### SYNTAX

[**no**] **area** *area-id* **range** *ip-address* **netmask** [**advertise** | **not-advertise**]

*area-id* - Identifies an area for which the routes are summarized. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

*ip-address* - Base address for the routes to summarize.

*netmask* - Network mask for the summary route.

**advertise** - Advertises the specified address range.

**not-advertise** - The summary is not sent, and the routes remain hidden from the rest of the network.

#### COMMAND MODE
Router Configuration

#### DEFAULT SETTING
Disabled

#### COMMAND USAGE
- This command can be used to summarize intra-area routes and advertise this information to other areas through Area Border Routers (ABRs).

- If the network addresses within an area are assigned in a contiguous manner, the ABRs can advertise a summary route that covers all of the individual networks within the area that fall into the specified range using a single **area range** command.

- If routes are set to be advertised by this command, the router will issue a Type 3 summary LSA for each address range specified by this command.

- This router supports up 64 summary routes for area ranges.

#### EXAMPLE
This example creates a summary address for all area routes in the range of 10.2.x.x.

```
Console(config-router)#area 10.2.0.0 range 10.2.0.0 255.255.0.0 advertise
Console(config-router)#
```

## auto-cost reference-bandwidth

Use this command to calculate the default metrics for an interface based on bandwidth. Use the **no** form to automatically assign costs based on interface type.

#### SYNTAX

**auto-cost reference-bandwidth** *reference-value*

**no auto-cost reference-bandwidth**

*reference-value* - Bandwidth of interface. (Range: 1-4294967 Mbps)

#### COMMAND MODE
Router Configuration

#### DEFAULT SETTING
1 Mbps

#### COMMAND USAGE
- The system calculates the cost for an interface by dividing the reference bandwidth by the interface bandwidth. By default, the cost is 1 Mbps for all port types (including 100 Mbps ports, 1 Gigabit ports, and 10 Gigabit ports).

- A higher reference bandwidth can be used for aggregate links to indicate preferred use as a lower cost interface.

- The ip ospf cost command overrides the cost calculated by the **auto-cost reference-bandwidth** command.

### EXAMPLE

This example sets the reference value to 10000, which generates a cost of 100 for 100 Mbps ports, 10 for 1 Gbps ports and 1 for 10 Gbps ports.

```
Console(config-router)#auto-cost reference-bandwidth 10000
Console(config-router)#
```

### RELATED COMMANDS

ip ospf cost (1156)

## default-metric

This command sets the default metric for external routes imported from other protocols. Use the **no** form to remove the default metric for the supported protocol types.

### SYNTAX

**default-metric** *metric-value*

**no default-metric**

*metric-value* – Metric assigned to all external routes imported from other protocols. (Range: 0-16777214)

### COMMAND MODE

Router Configuration

### DEFAULT SETTING

20

### COMMAND USAGE

- The default metric must be used to resolve the problem of redistributing external routes from other protocols that use incompatible metrics.

- This command does not override the metric value set by the redistribute command. When a metric value has not been configured by the redistribute command, the **default-metric** command sets the metric value to be used for all imported external routes.

### EXAMPLE

```
Console(config-router)#default-metric 100
Console(config-router)#
```

### RELATED COMMANDS

redistribute (1147)

## redistribute

This command redistributes external routing information from other routing protocols and static routes into an autonomous system. Use the **no** form to disable this feature or to restore the default settings.

### SYNTAX

**redistribute** {**connected** | **rip** | **static**} [**metric** *metric-value*] [**metric-type** *type-value*] **tag** *tag-value*]

**no redistribute** {**connected** | **rip** | **static**} [**metric**] [**metric-type** ] [**tag**]

**connected** - Imports all currently connected entries.

**rip** - Imports entries learned through the Routing Information Protocol.

**static** - Static routes will be imported into this Autonomous System.

*metric-value* - Metric assigned to all external routes for the specified protocol. (Range: 0-16777214: Default: 10)

*type-value*

**1** - Type 1 external route

**2** - Type 2 external route (default) - Routers do not add internal route metric to external route metric.

*tag-value* - A tag placed in the AS-external LSA to identify a specific external routing domain, or to pass additional information between routers. (Range: 0-4294967295)

### COMMAND MODE

Router Configuration

### DEFAULT SETTING

redistribution - none
metric-value - 10
type-metric - 2

### COMMAND USAGE

- This command is used to import routes learned from other routing protocols into the OSPF domain, and to generate AS-external-LSAs.

- When you redistribute external routes into an OSPF autonomous system (AS), the router automatically becomes an autonomous system boundary router (ASBR). If the **redistribute** command is used in conjunction with the default-information originate command to generate a “default” external route into the AS, the metric value specified in this command supersedes the metric specified in the default-information originate command.

- Metric type specifies the way to advertise routes to destinations outside the AS through External LSAs. When a Type 1 LSA is received by a router, it adds the internal cost to the external route metric. In other words, the cost of the route from any router within the AS is equal to the cost associated with reaching the advertising ASBR, plus the cost of the external route. When a Type 2 LSA is received by a router, it only uses the external route metric to determine route cost.

- A tag can be used to distinguish between routes learned from different external autonomous systems (other routing protocols). For example, if there are two ASBRs in a routing domain: A and B. ASBR A can be configured to redistribute routes learned from RIP domain 1 (identified by tag 1) and ASBR B can redistribute routes learned from RIP domain 2 (identified by tag 2).

### Example

This example redistributes routes learned from RIP as Type 1 external routes.

```
Console(config-router)#redistribute rip metric-type 1
Console(config-router)#
```

### Related Commands

default-information originate (1140)

## summary-address

This command aggregates routes learned from other protocols. Use the **no** form to remove a  summary address.

### Syntax

[**no**] **summary-address** *summary-address netmask*

*summary-address* - Summary address covering a range of addresses.

*netmask* - Network mask for the summary route.

### Command Mode

Router Configuration

### Default Setting

Disabled

### Command Usage

Redistributing routes from other protocols into OSPF normally requires the router to advertise each route individually in an external LSA. An Autonomous System Boundary Router (ASBR) can be configured to redistribute routes learned from other protocols by advertising an aggregate route into all attached autonomous systems. This helps both to decrease the number of external LSAs and the size of the OSPF link state database.

### Example

This example creates a summary address for all routes contained in 192.168.x.x.

```
Console(config-router)#summary-address 192.168.0.0 255.255.0.0
Console(config-router)#
```

### Related Commands

area range (1182)
redistribute (1184)

**area nssa** This command defines a not-so-stubby area (NSSA). To remove an NSSA, use the **no** form without any optional keywords. To remove an optional attribute, use the **no** form without the relevant keyword.

### SYNTAX

[**no**] **area** *area-id* **nssa**
[**translator-role** [**candidate** | **never** | **always**]] |
[**no-redistribution**] | [**no-summary**] | [**default-information-originate** [**metric** *metric-value* | **metric-type** *type-value*]]

*area-id* - Identifies the NSSA. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

**translator-role** - Indicates NSSA-ABR translator role for Type 5 external LSAs.

**candidate** - Router translates NSSA LSAs to Type-5 external LSAs if elected.

**never** - Router never translates NSSA LSAs to Type-5 external LSAs.

**always** - Router always translates NSSA LSAs to Type-5 external LSAs.

**no-redistribution** - Use this keyword when the router is an NSSA Area Border Router (ABR) and you want the redistribute command to import routes only into normal areas, and not into the NSSA. In other words, this keyword prevents the NSSA ABR from advertising external routing information (learned via routers in other areas) into the NSSA.

**no-summary** - Allows an area to retain standard NSSA features, but does not inject inter-area routes into this area.

**default-information-originate** - When the router is an NSSA Area Border Router (ABR) or an NSSA Autonomous System Boundary Router (ASBR), this parameter causes it to generate Type-7 default LSA into the NSSA. This default provides a route to other areas within the AS for an NSSA ABR, or to areas outside the AS for an NSSA ASBR.

**metric-value** - Metric assigned to Type-7 default LSAs.
(Range: 1-16777214: Default: 1)

**type-value**

**1** - Type 1 external route

**2** - Type 2 external route (default) - Routers do not add internal cost to the external route metric.

### COMMAND MODE

Router Configuration

### DEFAULT SETTING

No NSSA is configured.

### COMMAND USAGE

- All routers in a NSSA must be configured with the same area ID.

- An NSSA is similar to a stub, because when the router is an ABR, it can send a default route for other areas in the AS into the NSSA using the **default-**

**information-originate** keyword. However, an NSSA is different from a stub, because when the router is an ASBR, it can import a default external AS route (for routing protocol domains adjacent to the NSSA but not within the OSPF AS) into the NSSA using the **default-information-originate** keyword.

- External routes advertised into an NSSA can include network destinations outside the AS learned via OSPF, the default route, static routes, routes imported from other routing protocols such as RIP, and networks directly connected to the router that are not running OSPF.
- NSSA external LSAs (Type 7) are converted by any ABR adjacent to the NSSA into external LSAs (Type-5), and propagated into other areas within the AS.
- Also, note that unlike stub areas, all Type-3 summary LSAs are always imported into NSSAs to ensure that internal routes are always chosen over Type-7 NSSA external routes.
- This router supports up to 16 total areas (either normal transit areas, stubs, or NSSAs).

### EXAMPLE

This example creates a stub area 10.3.0.0, and assigns all interfaces with class B addresses 10.3.x.x to the NSSA. It also instructs the router to generate external LSAs into the NSSA when it is an NSSA ABR or NSSA ASBR.

```
Console(config-router)#area 10.3.0.0 nssa default-information-originate
Console(config-router)#network 10.3.0.0 255.255.0.0 area 10.2.0.0
Console(config-router)#
```

## area stub

This command defines a stub area. To remove a stub, use the **no** form without the optional keyword. To remove the summary attribute, use the **no** form with the summary keyword.

### SYNTAX

[**no**] **area** *area-id* **stub** [**no-summary**]

*area-id* - Identifies the stub area. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

**no-summary** - Stops an Area Border Router (ABR) from sending summary link advertisements into the stub area.

### COMMAND MODE

Router Configuration

### DEFAULT SETTING

No stub is configured.

Summary advertisement are sent into the stub.

#### COMMAND USAGE

- All routers in a stub must be configured with the same area ID.
- Routing table space is saved in a stub by blocking Type-4 AS summary LSAs and Type 5 external LSAs. The default setting for this command completely isolates the stub by blocking Type-3 summary LSAs that advertise the default route for destinations external to the local area or the autonomous system.
- Use the **no-summary** parameter of this command on the ABR attached to the stub to define a totally stubby area. Define an area as a totally stubby area only if routers in the area do not require summary LSAs from other areas.
- Use the area default-cost command to specify the cost of a default summary route sent into a stub by an ABR attached to the stub area.

#### EXAMPLE

This example creates a stub area 10.2.0.0, and assigns all interfaces with class B addresses 10.2.x.x to the stub.

```
Console(config-router)#area 10.2.0.0 stub
Console(config-router)#network 10.2.0.0 0.255.255.255 area 10.2.0.0
Console(config-router)#
```

#### RELATED COMMANDS

area default-cost (1144)

### area virtual-link

This command defines a virtual link. To remove a virtual link, use the **no** form with no optional keywords. To restore the default value for an attribute, use the **no** form with the required keyword.

#### SYNTAX

**area** *area-id* **virtual-link** *router-id*
[**authentication**] [**dead-interval** *seconds*] [**hello-interval** *seconds*]
[**retransmit-interval** *seconds*] [**transmit-delay** *seconds*]

**no area area-id virtual-link** *router-id*
[**authentication** | **dead-interval** | **hello-interval** | **retransmit-interval** |
**transmit-delay**]

**area** *area-id* **virtual-link** *router-id*
**authentication** [**message-digest** | **null**]
[**authentication-key** *key* | **message-digest-key** *key-id* **md5** *key*]

**no area** *area-id* **virtual-link** *router-id*
**authentication** [**authentication-key** |
**message-digest-key** *key-id*]

**area** *area-id* **virtual-link** *router-id*
[**authentication-key** *key* | **message-digest-key** *key-id* **md5** *key*]

**no area** *area-id* **virtual-link** *router-id*
[**authentication-key** | **message-digest-key** *key-id*]

*area-id* - Identifies the transit area for the virtual link.The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

*router-id* - Router ID of the virtual link neighbor. This specifies the Area Border Router (ABR) at the other end of the virtual link. To create a virtual link, enter this command for an ABR at both ends of the link. One of the ABRs must be next to the isolated area and the transit area at one end of the link, while the other ABR must be next to the transit area and backbone at the other end of the link.

**dead-interval** *seconds* - Specifies the time that neighbor routers will wait for a hello packet before they declare the router down. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 4 x hello interval, or 40 seconds)

**hello-interval** *seconds* - Specifies the transmit delay between sending hello packets. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase the routing traffic. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 10 seconds)

**retransmit-interval** *seconds* - Specifies the interval at which the ABR retransmits link-state advertisements (LSA) over the virtual link. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. However, note that this value should be larger for virtual links. (Range: 1-3600 seconds; Default: 5 seconds)

**transmit-delay** *seconds* - Estimates the time required to send a link-state update packet over the virtual link, considering the transmission and propagation delays. LSAs have their age incremented by this amount before transmission. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 1 second)

**authentication** - Specifies the authentication mode. If no optional parameters follow this keyword, then plain text authentication is used along with the password specified by the **authentication-key**. If **message-digest** authentication is specified, then the **message-digest-key** and **md5** parameters must also be specified. If the **null** option is specified, then no authentication is performed on any OSPF routing protocol messages.

**message-digest** - Specifies message-digest (MD5) authentication.

**null** - Indicates that no authentication is used.

**authentication-key** *key* - Sets a plain text password (up to 8 characters) that is used by neighboring routers on a virtual link to generate or verify the authentication field in protocol message headers. A separate password can be assigned to each network interface. However, this key must be the same for all neighboring routers on the same network (i.e., autonomous system). This key is only used when authentication is enabled for the backbone.

**message-digest-key** *key-id* **md5** *key* - Sets the key identifier and password to be used to authenticate protocol messages passed between neighboring routers and this router when using message digest (MD5) authentication. The *key-id* is an integer from 0-255, and the *key* is an alphanumeric string up to 16 characters long. If MD5 authentication is used on a virtual link, then it must be enabled on all routers within an autonomous system; and the key identifier and key must also be the same for all routers.

**COMMAND MODE**
Router Configuration

**DEFAULT SETTING**
*area-id*: None
*router-id*: None
hello-interval: 10 seconds
retransmit-interval: 5 seconds
transmit-delay: 1 second
dead-interval: 40 seconds
authentication-key: None
message-digest-key: None

**COMMAND USAGE**

- All areas must be connected to a backbone area (0.0.0.0) to maintain routing connectivity throughout the autonomous system. If it not possible to physically connect an area to the backbone, you can use a virtual link. A virtual link can provide a logical path to the backbone for an isolated area, or can be configured as a backup connection that can take over if the normal connection to the backbone fails.

- A virtual link can be configured between any two backbone routers that have an interface to a common non-backbone area. The two routers joined by a virtual link are treated as if they were connected by an unnumbered point-to-point network.

- Any area disconnected from the backbone must include the transit area ID and the router ID for a virtual link neighbor that is adjacent to the backbone.

**EXAMPLE**
This example creates a virtual link using the defaults for all optional parameters.

```
Console(config-router)#network 10.4.0.0 0.255.255.0.0 area 10.4.0.0
Console(config-router)#area 10.4.0.0 virtual-link 10.4.3.254
Console(config-router)#
```

This example creates a virtual link using MD5 authentication.

```
Console(config-router)#network 10.4.0.0 0.255.255.0.0 area 10.4.0.0
Console(config-router)#area 10.4.0.0 virtual-link 10.4.3.254 message-digest-key 5 md5 ld83jdpq
Console(config-router)#
```

**RELATED COMMANDS**
show ip protocols ospf (1175)

## network area

This command defines an OSPF area and the interfaces that operate within this area. Use the **no** form to disable OSPF for a specified interface.

#### SYNTAX

[**no**] **network** *ip-address netmask* **area** *area-id*

*ip-address* - Address of the interfaces to add to the area.

*netmask* - Network mask of the address range to add to the area.

*area-id* - Area to which the specified address or range is assigned. An OSPF area identifies a group of routers that share common routing information. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

#### COMMAND MODE

Router Configuration

#### DEFAULT SETTING

Disabled

#### COMMAND USAGE

- An area ID uniquely defines an OSPF broadcast area. The area ID 0.0.0.0 indicates the OSPF backbone for an autonomous system. Each router must be connected to the backbone via a direct connection or a virtual link.
- Set the area ID to the same value for all routers on a network segment using the network mask to add one or more interfaces to an area.
- If an address range is overlapped in subsequent network area commands, the router will use the network area with the address range that most closely matches the interface address. Also, note that if a more specific address range is removed from an area, the interface belonging to that range may still remain active if a less specific address range covering that area has been specified.

#### EXAMPLE

This example creates the backbone 0.0.0.0 covering class B addresses 10.1.x.x, and a normal transit area 10.2.9.0 covering the class C addresses 10.2.9.x.

```
Console(config-router)#network 10.1.0.0 255.255.0.0 area 0.0.0.0
Console(config-router)#network 10.2.9.0 255.255.255.0 area 10.1.0.0
Console(config-router)#
```

### ip ospf authentication

This command specifies the authentication type used for an interface. Enter this command without any optional parameters to specify plain text (or simple password) authentication. Use the **no** form to restore the default of no authentication.

#### SYNTAX

**ip ospf** [*ip-address*] **authentication** [**message-digest** | **null**]

**no ip ospf** [*ip-address*] **authentication**

*ip-address* - IP address of the interface. Enter this parameter to specify a unique authentication type for a primary or secondary IP address associated with the current VLAN. If not specified, the command applies to all networks connected to the current interface.

**message-digest** - Specifies message-digest (MD5) authentication.

**null** - Indicates that no authentication is used.

### COMMAND MODE

Interface Configuration (VLAN)

### DEFAULT SETTING

No authentication

### COMMAND USAGE

- Use authentication to prevent routers from inadvertently joining an unauthorized area. Configure routers in the same area with the same password or key. All neighboring routers on the same network with the same password will exchange routing data.
- This command creates a password (key) that is inserted into the OSPF header when routing protocol packets are originated by this device. Assign a separate password to each network for different interfaces.
- When using simple password authentication, a password is included in the packet. If it does not match the password configured on the receiving router, the packet is discarded. This method provides very little security as it is possible to learn the authentication key by snooping on routing protocol packets.
- When using Message-Digest 5 (MD5) authentication, the router uses the MD5 algorithm to verify data integrity by creating a 128-bit message digest from the authentication key. Without the proper key and key-id, it is nearly impossible to produce any message that matches the pre-specified target message digest.
- Before specifying plain-text password authentication for an interface, configure a password with the ip ospf authentication-key command. Before specifying MD5 authentication for an interface, configure the message-digest key-id and key with the ip ospf message-digest-key command.
- The plain-text authentication-key, or the MD5 *key-id* and *key*, must be used consistently throughout the autonomous system.

### EXAMPLE

This example enables message-digest authentication for the specified interface.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf authentication message-digest
Console(config-if)#
```

### RELATED COMMANDS

ip ospf authentication-key (1156)
ip ospf message-digest-key (1159)

## ip ospf authentication-key

This command assigns a simple password to be used by neighboring routers to verify the authenticity of routing protocol messages. Use the **no** form to remove the password.

### SYNTAX

**ip ospf** [*ip-address*] **authentication-key** *key*

**no ip ospf** [*ip-address*] **authentication-key**

*ip-address* - This parameter can be used to indicate a specific IP address connected to the current interface. If not specified, the command applies to all networks connected to the current interface.

*key* - Sets a plain text password. (Range: 1-8 characters)

### COMMAND MODE

Interface Configuration (VLAN)

### DEFAULT SETTING

No password

### COMMAND USAGE

- Before specifying plain-text password authentication for an interface with the ip ospf authentication command, configure a password with this command.
- This command creates a password (key) that is inserted into the OSPF header when routing protocol packets are originated by this device. Assign a separate password to each network for different interfaces. All neighboring routers on the same network with the same password will exchange routing data.
- A different password can be assigned to each network interface, but the password must be used consistently on all neighboring routers throughout a network (i.e., autonomous system).

### EXAMPLE

This example sets a password for the specified interface.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf authentication-key badboy
Console(config-if)#
```

### RELATED COMMANDS

ip ospf authentication (1154)

## ip ospf cost

This command explicitly sets the cost of sending a protocol packet on an interface, where higher values indicate slower ports. Use the **no** form to restore the default value.

### SYNTAX

**ip ospf** [*ip-address*] **cost** *cost*

**no ip ospf** [*ip-address*] **cost**

*ip-address* - This parameter can be used to indicate a specific IP address connected to the current interface. If not specified, the command applies to all networks connected to the current interface.

*cost* - Link metric for this interface. Use higher values to indicate slower ports. (Range: 1-65535)

#### COMMAND MODE
Interface Configuration (VLAN)

#### DEFAULT SETTING
1

#### COMMAND USAGE
- The interface cost indicates the overhead required to send packets across a certain interface. This is advertised as the link cost in router link state advertisements.
- Routes are assigned a metric equal to the sum of all metrics for each interface link in the route.
- This router uses a default cost of 1 for all port types. Therefore, if any VLAN contains 10 Gbps ports, you may want to reset the cost for other VLANs which do not contain 10 Gbps ports to a value greater than 1.

#### EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf cost 10
Console(config-if)#
```

### ip ospf dead-interval

This command sets the interval at which hello packets are not seen before neighbors declare the router down. Use the **no** form to restore the default value.

#### SYNTAX

**ip ospf** [*ip-address*] **dead-interval** *seconds*

**no ip ospf** [*ip-address*] **dead-interval**

*ip-address* - This parameter can be used to indicate a specific IP address connected to the current interface. If not specified, the command applies to all networks connected to the current interface.

*seconds* - The maximum time that neighbor routers can wait for a hello packet before declaring the transmitting router down. This interval must be set to the same value for all routers on the network. (Range: 1-65535)

#### COMMAND MODE
Interface Configuration (VLAN)

#### DEFAULT SETTING

40, or four times the interval specified by the ip ospf hello-interval command.

#### COMMAND USAGE

The dead-interval is advertised in the router's hello packets. It must be a multiple of the hello-interval and be the same for all routers on a specific network.

#### EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf dead-interval 50
Console(config-if)#
```

#### RELATED COMMANDS

ip ospf hello-interval (1158)

## ip ospf hello-interval

This command specifies the interval between sending hello packets on an interface. Use the **no** form to restore the default value.

#### SYNTAX

**ip ospf** [ip-address] **hello-interval** *seconds*

**no ip ospf** [*ip-address*] **hello-interval**

*ip-address* - This parameter can be used to indicate a specific IP address connected to the current interface. If not specified, the command applies to all networks connected to the current interface.

*seconds* - Interval at which hello packets are sent from an interface. This interval must be set to the same value for all routers on the network. (Range: 1-65535)

#### COMMAND MODE

Interface Configuration (VLAN)

#### DEFAULT SETTING

10 seconds

#### COMMAND USAGE

Hello packets are used to inform other routers that the sending router is still active. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase routing traffic.

#### EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf hello-interval 5
Console(config-if)#
```

### ip ospf message-digest-key

This command enables message-digest (MD5) authentication on the specified interface and to assign a key-id and key to be used by neighboring routers. Use the **no** form to remove an existing key.

#### SYNTAX

**ip ospf** [*ip-address*] **message-digest-key** *key-id* **md5** *key*

**no ip ospf** [*ip-address*] **message-digest-key** *key-id*

*ip-address* - This parameter can be used to indicate a specific IP address connected to the current interface. If not specified, the command applies to all networks connected to the current interface.

*key-id* - Index number of an MD5 key. (Range: 0-255)

*key* - Alphanumeric password used to generate a 128 bit message digest or “fingerprint.” (Range: 1-16 characters)

#### COMMAND MODE

Interface Configuration (VLAN)

#### DEFAULT SETTING

MD5 authentication is disabled.

#### COMMAND USAGE

- Before specifying MD5 authentication for an interface with the ip ospf authentication command, configure the message-digest key-id and key with this command.

- Normally, only one key is used per interface to generate authentication information for outbound packets and to authenticate incoming packets. Neighbor routers must use the same key identifier and key value.

- When changing to a new key, the router will send multiple copies of all protocol messages, one with the old key and another with the new key. Once all the neighboring routers start sending protocol messages back to this router with the new key, the router will stop using the old key. This rollover process gives the network administrator time to update all the routers on the network without affecting the network connectivity. Once all the network routers have been updated with the new key, the old key should be removed for security reasons.

#### EXAMPLE

This example sets a message-digest key identifier and password.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf message-digest-key 1 md5 aiebel
Console(config-if)#
```

#### RELATED COMMANDS

ip ospf authentication (1154)

## ip ospf priority

This command sets the router priority used when determining the designated router (DR) and backup designated router (BDR) for an area. Use the **no** form to restore the default value.

### SYNTAX

**ip ospf** [*ip-address*] **priority** *priority*

**no ip ospf** [*ip-address*] **priority**

*ip-address* - This parameter can be used to indicate a specific IP address connected to the current interface. If not specified, the command applies to all networks connected to the current interface.

*priority* - Sets the interface priority for this router. (Range: 0-255)

### COMMAND MODE

Interface Configuration (VLAN)

### DEFAULT SETTING

1

### COMMAND USAGE

- A designated router (DR) and backup designated router (BDR) are elected for each OSPF network segment based on Router Priority. The DR forms an active adjacency to all other routers in the network segment to exchange routing topology information. If for any reason the DR fails, the BDR takes over this role.

- Set the priority to zero to prevent a router from being elected as a DR or BDR. If set to any value other than zero, the router with the highest priority will become the DR and the router with the next highest priority becomes the BDR. If two or more routers are tied with the same highest priority, the router with the higher ID will be elected.

- If a DR already exists for a network segment when this interface comes up, the new router will accept the current DR regardless of its own priority. The DR will not change until the next time the election process is initiated.

- Configure router priority for multi-access networks only and not for point-to-point networks.

### EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf priority 5
Console(config-if)#
```

## ip ospf retransmit-interval

This command specifies the time between resending link-state advertisements (LSAs). Use the **no** form to restore the default value.

### SYNTAX

**ip ospf** [*ip-address*] **retransmit-interval** *seconds*

**no ip ospf** [*ip-address*] **retransmit-interval**

*ip-address* - This parameter can be used to indicate a specific IP address connected to the current interface. If not specified, the command applies to all networks connected to the current interface.

*seconds* - Sets the interval at which LSAs are retransmitted from this interface. (Range: 1-65535)

### COMMAND MODE
Interface Configuration (VLAN)

### DEFAULT SETTING
5 seconds

### COMMAND USAGE
- A router will resend an LSA to a neighbor if it receives no acknowledgment after the specified retransmit interval. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. Note that this value should be larger for virtual links.
- Set this interval to a value that is greater than the round-trip delay between any two routers on the attached network to avoid unnecessary retransmissions.

### EXAMPLE
```
Console(config)#interface vlan 1
Console(config-if)#ip ospf retransmit-interval 7
Console(config-if)#
```

## ip ospf transmit-delay

This command sets the estimated time to send a link-state update packet over an interface. Use the **no** form to restore the default value.

### SYNTAX
**ip ospf** [*ip-address*] **transmit-delay** *seconds*

**no ip ospf** [*ip-address*] **transmit-delay**

*ip-address* - This parameter can be used to indicate a specific IP address connected to the current interface. If not specified, the command applies to all networks connected to the current interface.

*seconds* - Sets the estimated time required to send a link-state update. (Range: 1-65535)

### COMMAND MODE
Interface Configuration (VLAN)

### DEFAULT SETTING
1 second

#### Command Usage

- LSAs have their age incremented by this delay before transmission. When estimating the transmit delay, consider both the transmission and propagation delays for an interface. Set the transmit delay according to link speed, using larger values for lower-speed links.

- If this delay is not added, the time required to transmit an LSA over the link is not taken into consideration by the routing process. On slow links, the router may send packets more quickly than devices can receive them. To avoid this problem, use the transmit delay to force the router to wait a specified interval between transmissions.

#### Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf transmit-delay 6
Console(config-if)#
```

### passive-interface

This command suppresses OSPF routing traffic on the specified interface. Use the **no** form to allow routing traffic to be sent and received on the specified interface.

#### Syntax

[**no**] **passive-interface vlan** *vlan-id* [*ip-address*]

*vlan-id* - VLAN ID. (Range: 1-4093)

*ip-address* - An IPv4 address configured on this interface.

#### Command Mode

Router Configuration

#### Default Setting

None

#### Command Usage

You can configure an OSPF interface as passive to prevent OSPF routing traffic from exiting or entering that interface. No OSPF adjacency can be formed if one of the interfaces involved is set to passive mode. The specified interface will appear as a stub in the OSPF domain. Also, if you configure an OSPF interface as passive where an adjacency already exists, the adjacency will drop almost immediately.

#### Example

```
Console(config-router)#passive-interface vlan 1
Console(config-router)#
```

### show ip ospf

This command shows basic information about the routing configuration.

### SYNTAX

**show ip ospf** [*process-id*]

*process-id* - The ID of the router process for which information will be displayed. (Range: 1-65535)

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show ip ospf
 Routing Process "ospf 1" with ID 192.168.1.3
 Process uptime is 20 minutes
 Conforms to RFC2328, and RFC1583Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Refresh timer 10 secs
 Number of incoming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 LSDB database overflow limit is 20480
 Number of LSA originated 1
 Number of LSA received 0
 Number of areas attached to this router: 1

   Area 192.168.1.3
     Number of interfaces in this area is 1(1)
     Number of fully adjacent neighbors in this area is 0
     Area has no authentication
     SPF algorithm last executed 00:00:08.739 ago
     SPF algorithm executed 1 times
     Number of LSA 1. Checksum 0x007f09
Console#
```

**Table 5: show ip ospf** - display description

| Field | Description |
|---|---|
| Routing Process with ID | OSPF process ID and router ID. The router ID uniquely identifies the router in the autonomous system. By convention, this is normally set to one of the router's IP interface addresses. |
| Process uptime | The time this process has been running |
| Conforms to RFC2328 | Shows that this router is compliant with OSPF Version 2. |
| RFC1583 Compatibility flag | Shows whether or not compatibility with the RFC 1583 (an earlier version of OSPFv2) is enabled. |
| Supports only single TOS (TOS0) routes | Optional Type of Service (ToS) specified in OSPF Version 2, Appendix F.1.2 is not supported, so only one cost per interface can be assigned. |
| SPF schedule delay | Delay between receiving a change to SPF calculation. |
| Hold time | Sets the hold time between two consecutive SPF calculations. |
| Refresh timer | The time between refreshing the LSA database. |
| Number of current DD exchange neighbors | Number of neighbors currently exchanging database descriptor packets. |

**Table 5: show ip ospf** - display description (Continued)

| Field | Description |
|---|---|
| Number of external LSA | The number of external link-state advertisements (Type 5 LSAs) in the link-state database. These LSAs advertise information about routes outside of the autonomous system. |
| Checksum | The sum of the LS checksums of the external link-state advertisements contained in the link-state database. |
| Number of opaque AS LSA | Number of opaque link-state advertisements (Type 9, 10 and 11 LSAs) in the link-state database. These LSAs advertise information about external applications, and are only used by OSPF for the graceful restart process. |
| Checksum | The sum of the LS checksums of opaque link-state advertisements contained in the link-state database. |
| LSDB database overflow limit | The maximum number of LSAs allowed in the external database. |
| Number of LSA originated | The number of new link-state advertisements that have been originated. |
| Number of LSA received | The number of link-state advertisements that have been received. |
| Number of areas attached to this router | The number of configured areas attached to this router. |
| Number of interfaces in this area is | The number of interfaces attached to this area |
| Number of fully adjacent neighbors in this area is | The number of neighbors for which the exchange of recognition protocol messages has been completed and are now fully adjacent |
| Area has (no) authentication | Shows whether or not the authentication has been enabled |
| SPF algorithm last executed | The last time the shortest path first algorithm was executed |
| SPF algorithm executed x times | The number of times the shortest path first algorithm has been executed for this area |
| Number of LSA | The number of new link-state advertisements that have been originated. |
| Checksum | The sum of the link-state advertisements' LS checksums contained in this area's link-state database. |

## show ip ospf border-routers

This command shows entries in the routing table that lead to an Area Border Router (ABR) or Autonomous System Boundary Router (ASBR).

### SYNTAX

**show ip ospf** [*process-id*] **border-routers**

*process-id* - The ID of the router process for which information will be displayed. (Range: 1-65535)

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show ip ospf border-routers

OSPF process 1 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 192.168.0.3 [1] via 192.168.0.3, vlan1, ABR, ASBR, Area 0.0.0.0
Console#
```

## show ip ospf database

This command shows information about different OSPF Link State Advertisements (LSAs) stored in this router's database.

### SYNTAX

**show ip ospf** [*process-id*] **database**
[**asbr-summary** | **external** | **network** | **nssa-external** | **router** | **summary**]
[**adv-router** *ip-address* | *link-state-id* | **self-originate**]

*process-id* - The ID of the router process for which information will be displayed. (Range: 1-65535)

**adv-router** - IP address of the advertising router. If not entered, information about all advertising routers is displayed.

*ip-address* - IP address of the specified router. If no address is entered, information about the local router is displayed.

*link-state-id* - The network portion described by an LSA. The *link-state-id* entered should be:

- An IP network number for Type 3 Summary and External LSAs
- A Router ID for Router, Network, and Type 4 AS Summary LSAs

Also, note that when an Type 5 ASBR External LSA is describing a default route, its *link-state-id* is set to the default destination (0.0.0.0).

**self-originate** - Shows LSAs originated by this router.

**asbr-summary** - Shows information about Autonomous System Boundary Router summary LSAs.

**external** - Shows information about external LSAs.

**network** - Shows information about network LSAs.

**nssa-external** - Shows information about NSSA external LSAs.

**router** - Shows information about router LSAs.

**summary** - Shows information about summary LSAs.

### COMMAND MODE

Privileged Exec

### EXAMPLES

The following shows output for the **show ip ospf database** command.

```
Console#show ip ospf database

            OSPF Router with ID (192.168.0.2) (Process ID 1)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
192.168.0.2     192.168.0.2     225 0x80000004 0xdac5 1
192.168.0.3     192.168.0.3     220 0x80000004 0xd8c4 1

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
192.168.0.2     192.168.0.2     225 0x80000001 0x9c0f

                AS External Link States

Link ID         ADV Router      Age  Seq#       CkSum  Route            Tag
0.0.0.0         192.168.0.2     487 0x80000001 0xd491 E2 0.0.0.0/0 0
0.0.0.0         192.168.0.3     222 0x80000001 0xce96 E2 0.0.0.0/0 0

Console#
```

**Table 6: show ip ospf database** - display description

| Field | Description |
|---|---|
| OSPF Router Process with ID | OSPF process ID and router ID. The router ID uniquely identifies the router in the autonomous system. By convention, this is normally set to one of the router's IP interface addresses. |
| Link ID | Either a Router ID or an IP Address; it identifies the piece of the routing domain that is being described by the advertisement |
| ADV Router | Advertising router ID |
| Age | Age of LSA (in seconds) |
| Seq# | Sequence number of LSA (used to detect older duplicate LSAs) |
| CkSum | Checksum of the complete contents of the LSA |
| Link count | Number of interfaces attached to the router |
| Route | Type 1 or Type 2 external metric (see the redistribute command) and route |
| Tag | Optional tag if defined (see the redistribute command) |

The following shows output when using the **asbr-summary** keyword.

```
Console#show ip ospf database asbr-summary

            OSPF Router with ID (0.0.0.0) (Process ID 1)

                ASBR-Summary Link States (Area 0.0.0.1)

  LS age: 0
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: ASBR-summary-LSA
  Link State ID: 2.1.0.0 (AS Boundary Router address)
```

```
  Advertising Router: 192.168.2.1
  LS Seq Number: 80000001
  Checksum: 0x7b67
  Length: 28
  Network Mask: /0
        TOS: 0  Metric: 10

Console#
```

**Table 7: show ip ospf database summary** - display description

| Field | Description |
|---|---|
| OSPF Router ID | Router ID |
| LS age | Age of LSA (in seconds) |
| Options | Optional capabilities associated with the LSA |
| LS Type | Summary Links - LSA describes routes to AS boundary routers |
| Link State ID | Interface address of the autonomous system boundary router |
| Advertising Router | Advertising router ID |
| LS Sequence Number | Sequence number of LSA (used to detect older duplicate LSAs) |
| Checksum | Checksum of the complete contents of the LSA |
| Length | The length of the LSA in bytes |
| Network Mask | Address mask for the network |
| TOS | Type of Service – This router only supports TOS 0 (or normal service) |
| Metric | Cost of the link |

The following shows output when using the **external** keyword.

```
Console#show ip ospf database external
OSPF Router process 100 with ID (10.10.11.50)
AS External Link States LS age: 298
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 10.10.100.0 (External Network Number)
Advertising Router: 10.10.11.50
LS Seq Number: 80000001
Checksum: 0x7033
Length: 36
Network Mask: /24
Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 20
Forward Address: 10.10.11.50
External Route Tag: 0


            OSPF Router with ID (0.0.0.0) (Process ID 1)

                AS External Link States

  LS age: 0
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: AS-external-LSA
```

```
   Link State ID: 0.0.0.0 (External Network Number)
   Advertising Router: 192.168.0.2
   LS Seq Number: 80000005
   Checksum: 0xcc95
   Length: 36
   Network Mask: /0
         Metric Type: 2 (Larger than any link state path)
         TOS: 0
         Metric: 1
         Forward Address: 0.0.0.0
         External Route Tag: 0

Console#
```

**Table 8: show ip ospf database external** - display description

| Field | Description |
|---|---|
| OSPF Router ID | Router ID |
| LS age | Age of LSA (in seconds) |
| Options | Optional capabilities associated with the LSA |
| LS Type | AS External Links - LSA describes routes to destinations outside the AS (including default external routes for the AS) |
| Link State ID | IP network number (External Network Number) |
| Advertising Router | Advertising router ID |
| LS Sequence Number | Sequence number of LSA (used to detect older duplicate LSAs) |
| Checksum | Checksum of the complete contents of the LSA |
| Length | The length of the LSA in bytes |
| Network Mask | Address mask for the network |
| Metric Type | Type 1 or Type 2 external metric (see the redistribute command) |
| TOS | Type of Service – This router only supports TOS 0 (or normal service) |
| Metric | Cost of the link |
| Forward Address | Next hop address. If this field is set to 0.0.0.0, data is forwarded to the originator of the advertisement. |
| External Route Tag | Optional tag if defined (see the redistribute command) |

The following shows output when using the **network** keyword.

```
Console#show ip ospf database network

            OSPF Router with ID (0.0.0.0) (Process ID 1)

                Net Link States (Area 0.0.0.0)

   LS age: 0
   Options: 0x2 (*|-|-|-|-|-|E|-)
   LS Type: network-LSA
   Link State ID: 192.168.0.2 (address of Designated Router)
   Advertising Router: 192.168.0.2
   LS Seq Number: 80000005
   Checksum: 0x9413
```

```
 Length: 32
 Network Mask: /24
       Attached Router: 192.168.0.2
       Attached Router: 192.168.0.3
.
.
.
```

**Table 9: show ip ospf database network** - display description

| Field | Description |
|---|---|
| OSPF Router ID | Router ID |
| LS age | Age of LSA (in seconds) |
| Options | Optional capabilities associated with the LSA |
| LS Type | Network Link - LSA describes the routers attached to the network |
| Link State ID | Interface address of the designated router |
| Advertising Router | Advertising router ID |
| LS Sequence Number | Sequence number of LSA (used to detect older duplicate LSAs) |
| Checksum | Checksum of the complete contents of the LSA |
| Length | The length of the LSA in bytes |
| Network Mask | Address mask for the network |
| Attached Router | List of routers attached to the network; i.e., fully adjacent to the designated router, including the designated router itself |

The following shows output when using the **router** keyword.

```
Console#show ip ospf database router

            OSPF Router with ID (0.0.0.0) (Process ID 1)

                Router Link States (Area 0.0.0.0)

 LS age: 0
 Options: 0x2 (*|-|-|-|-|-|E|-)
 Flags: 0x2 : ASBR
 LS Type: router-LSA
 Link State ID: 192.168.0.2
 Advertising Router: 192.168.0.2
 LS Seq Number: 80000008
 Checksum: 0xd2c9
 Length: 36
   Link connected to: a Transit Network
    (Link ID) Designated Router address: 192.168.0.2
    (Link Data) Router Interface address: 192.168.0.2
     Number of TOS metrics: 0
     TOS 0 Metric: 1
.
.
.
```

**Table 10: show ip ospf database router** - display description

| Field | Description |
|---|---|
| OSPF Router ID | Router ID |
| LS age | Age of LSA (in seconds) |
| Options | Optional capabilities associated with the LSA |
| Flags | Indicate if this router is a virtual link endpoint, an ASBR, or an ABR |
| LS Type | Router Link - LSA describes the router's interfaces. |
| Link State ID | Router ID of the router that originated the LSA |
| Advertising Router | Advertising router ID |
| LS Sequence Number | Sequence number of LSA (used to detect older duplicate LSAs) |
| Checksum | Checksum of the complete contents of the LSA |
| Length | The length of the LSA in bytes |
| Link connected to | Link-state type, including transit network, stub network, or virtual link |
| Link ID | Link type and corresponding Router ID or network address |
| Link Data | ◆ Router ID for transit network<br>◆ Network's IP address mask for stub network<br>◆ Neighbor Router ID for virtual link |
| Number of TOS metrics | Type of Service metric – This router only supports TOS 0 (or normal service) |
| TOS | Type of Service – This router only supports TOS 0 (or normal service) |
| Metric | Cost of the link |

The following shows output when using the **summary** keyword.

```
Console#show ip ospf database summary

          OSPF Router with ID (0.0.0.0) (Process ID 1)

             Summary Link States (Area 0.0.0.0)

 LS age: 1
 Options: 0x0 (*|-|-|-|-|-|-|-)
 LS Type: summary-LSA
 Link State ID: 192.168.10.0 (summary Network Number)
 Advertising Router: 2.1.0.0
 LS Seq Number: 80000005
 Checksum: 0x479d
 Length: 28
 Network Mask: /24
      TOS: 0  Metric: 0
⋮
```

**Table 11: show ip ospf database summary** - display description

| Field | Description |
|---|---|
| OSPF Router ID | Router ID |
| LS age | Age of LSA (in seconds) |
| Options | Optional capabilities associated with the LSA |
| LS Type | Summary Links - LSA describes routes to networks |
| Link State ID | Router ID of the router that originated the LSA |
| Advertising Router | Advertising router ID |
| LS Sequence Number | Sequence number of LSA (used to detect older duplicate LSAs) |
| Checksum | Checksum of the complete contents of the LSA |
| Length | The length of the LSA in bytes |
| Network Mask | Destination network's IP address mask |
| Metrics | Cost of the link |

## show ip ospf interface

This command displays summary information for OSPF interfaces.

### SYNTAX

**show ip ospf interface** [**vlan** *vlan-id*]

*vlan-id* - VLAN ID (Range: 1-4093)

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show ip ospf interface vlan 1
VLAN1 is up, line protocol is up
  Internet Address 192.168.0.2/24, Area 0.0.0.0, MTU 1500
  Process ID 1, Router ID 192.168.0.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.0.2, Interface Address 192.168.0.2
  Backup Designated Router (ID) 192.168.0.3, Interface Address 192.168.0.3
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:10
  Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 920 sent 975, DD received 5 sent 4
  LS-Req received 1 sent 1, LS-Upd received 14 sent 18
  LS-Ack received 17 sent 13, Discarded 0
Console#
```

**Table 12: show ip ospf interface** - display description

| Field | Description |
|---|---|
| VLAN | VLAN ID and Status of physical link |
| Internet Address | IP address of OSPF interface |

**Table 12: show ip ospf interface** - display description (Continued)

| Field | Description |
|---|---|
| Area | OSPF area to which this interface belongs |
| MTU | Maximum transfer unit |
| Process ID | OSPF process ID |
| Router ID | Router ID |
| Network Type | Includes broadcast, non-broadcast, or point-to-point networks |
| Cost | Interface transmit cost |
| Transmit Delay | Interface transmit delay (in seconds) |
| State | ◆ Disabled – OSPF not enabled on this interface<br>◆ Down – OSPF is enabled on this interface, but interface is down<br>◆ Loopback – This is a loopback interface<br>◆ Waiting – Router is trying to find the DR and BDR<br>◆ DR – Designated Router<br>◆ BDR – Backup Designated Router<br>◆ DRother – Interface is on a multiaccess network, but is not the DR or BDR |
| Priority | Router priority |
| Designated Router | Designated router ID and respective interface address |
| Backup Designated Router | Backup designated router ID and respective interface address |
| Timer intervals | Configuration settings for timer intervals, including Hello, Dead and Retransmit |
| Neighbor Count | Count of network neighbors and adjacent neighbors |
| Adjacent neighbor count | Count of adjacent neighbors |
| Hello | Number of Hello LSAs received and sent |
| DD | Number of Database Descriptor packets received and sent. |
| LS-Req | Number of LSA requests |
| LS-Upd | Number of LSA updates |
| LS-Ack | Number of LSA acknowledgements |
| Discarded | Number of LSAs discarded |

## show ip ospf neighbor

This command displays information about neighboring routers on each interface within an OSPF area.

### SYNTAX

**show ip ospf** [*process-id*] **neighbor**

*process-id* - The ID of the router process for which information will be displayed. (Range: 1-65535)

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show ip ospf neighbor

     ID        Pri      State          Address       Interface
--------------- ------ ---------------- --------------- --------------
   192.168.0.3      1        FULL/BDR     192.168.0.3         vlan1
Console#
```

**Table 13: show ip ospf neighbor** - display description

| Field | Description |
|---|---|
| Neighbor ID | Neighbor's router ID |
| Pri | Neighbor's router priority |
| State | OSPF state and identification flag<br>States include:<br>Down – Connection down<br>Attempt – Connection down, but attempting contact (for non-broadcast networks)<br>Init – Have received Hello packet, but communications not yet established<br>Two-way – Bidirectional communications established<br>ExStart – Initializing adjacency between neighbors<br>Exchange – Database descriptions being exchanged<br>Loading – LSA databases being exchanged<br>Full – Neighboring routers now fully adjacent<br>Identification flags include:<br>D – Dynamic neighbor<br>S – Static neighbor<br>DR – Designated router<br>BDR – Backup designated router |
| Address | IP address of this interface |
| Interface | The interface to which this neighbor is attached |

## show ip ospf route

This command displays the OSPF routing table.

### SYNTAX

**show ip ospf** [*process-id*] **route**

*process-id* - The ID of the router process for which information will be displayed. (Range: 1-65535)

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show ip ospf route
OSPF process 1:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
O  10.10.0.0/24 [10] is directly connected, fe1/1, Area 0.0.0.0
O  10.10.11.0/24 [10] is directly connected, fe1/2, Area 0.0.0.0
O  10.10.11.100/32 [10] is directly connected, lo, Area 0.0.0.0
E2 10.15.0.0/24 [10/50] via 10.10.0.1, vlan1
IA 172.16.10.0/24 [30] via 10.10.11.50, vlan2, Area 0.0.0.0
```

```
E2 192.168.0.0/16 [10/20] via 10.10.11.50, vlan2

Console#
```

## show ip ospf virtual-links

This command displays detailed information about virtual links.

### SYNTAX

**show ip ospf virtual-links**

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show ip ospf virtual-links
Virtual Link VLINK1 to router 192.168.0.2 is up
  Transit area 0.0.0.1 via interface vlan1
  Local address 192.168.0.3
  Remote address 192.168.0.2
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
    Adjacency state Down
Console#
```

**Table 14: show ip ospf neighbor** - display description

| Field | Description |
|---|---|
| Virtual Link to router | OSPF neighbor and link state (up or down) |
| Transit area | Common area the virtual link crosses to reach the target router |
| Local address | The IP address of ABR that serves as an endpoint connecting the isolated area to the common transit area. |
| Remote address | The IP address this virtual neighbor is using. The neighbor must be an ABR at the other endpoint connecting the common transit area to the backbone itself. |
| Transmit Delay | Estimated transmit delay (in seconds) on the virtual link |
| Timer intervals | Configuration settings for timer intervals, including Hello, Dead and Retransmit |

### RELATED COMMANDS

area virtual-link (1151)

### show ip protocols ospf

This command displays OSPF process parameters.

#### SYNTAX

**show ip ospf virtual-links**

#### COMMAND MODE

Privileged Exec

#### EXAMPLE

```
Console#show ip protocols ospf
Routing Protocol is "ospf 200"
Redistributing: rip
Routing for Networks:
192.30.30.0/24
192.40.40.0/24
  Routing for Summary Address:
    192.168.1.0/24
    192.168.3.0/24
Distance: (default is 110)
Console#
```

**Table 15: show ip protocols ospf** - display description

| Field | Description |
|---|---|
| Routing Protocol | Name and autonomous system number of this OSPF process. |
| Redistributing | Shows if route redistribution has been enabled with the redistribute command. |
| Routing for Networks | Networks for which the OSPF is currently registering routing information. |
| Routing for Summary Address | Shows the networks for which route summarization is in effect |
| Distance | The administrative distance used for external routes learned by OSPF (see the ip route command). |

## OPEN SHORTEST PATH FIRST (OSPFV3)

**Table 16: Open Shortest Path First Commands** (Version 3)

| Command | Function | Mode |
|---|---|---|
| *General Configuration* | | |
| router ipv6 ospf | Enables or disables OSPFv3 routing process | GC |
| abr-type | Sets the criteria used to determine if this router can declare itself an ABR and issue Type 3 and Type 4 summary LSAs | RC |
| max-current-dd | Sets the maximum number of neighbors with which the switch can concurrently exchange database descriptor packets | RC |
| router-id | Sets the router ID for this device | RC |
| timers spf | Configures the delay after a topology change and the hold time between consecutive SPF calculations | RC |
| *Route Metrics and Summaries* | | |

**Table 16: Open Shortest Path First Commands** (Version 3) **(Continued)**

| Command | Function | Mode |
|---|---|---|
| area default-cost | Sets the cost for a default summary route sent into a stub | RC |
| area range | Summarizes routes advertised by an ABR | RC |
| default-metric | Sets the default metric for external routes imported from other protocols | RC |
| redistribute | Redistribute routes from one routing domain to another | RC |
| *Area Configuration* | | |
| area stub | Defines a stubby area that cannot send or receive LSAs | RC |
| area virtual-link | Defines a virtual link from an area border routers to the backbone | RC |
| ipv6 router ospf area | Binds an area to the selected interface | IC |
| ipv6 router ospf tag area | Binds an area to the selected interface and process | IC |
| *Interface Configuration* | | |
| ipv6 ospf cost | Specifies the cost of sending a packet on an interface | IC |
| ipv6 ospf dead-interval | Sets the interval at which hello packets are not seen before neighbors declare the router down | IC |
| ipv6 ospf hello-interval | Specifies the interval between sending hello packets | IC |
| ipv6 ospf priority | Sets the router priority used to determine the designated router | IC |
| ipv6 ospf retransmit-interval | Specifies the time between resending a link-state advertisement | IC |
| ipv6 ospf transmit-delay | Estimates time to send a link-state update packet over an interface | IC |
| passive-interface | Suppresses OSPF routing traffic on the specified interface | RC |
| *Display Information* | | |
| show ipv6 ospf | Displays general information about the routing processes | PE |
| show ipv6 ospf database | Shows information about different LSAs in the database | PE |
| show ipv6 ospf interface | Displays interface information | PE |
| show ipv6 ospf neighbor | Displays neighbor information | PE |
| show ipv6 ospf route | Displays the OSPF routing table | PE |
| show ipv6 ospf virtual-links | Displays parameters and the adjacency state of virtual links | PE |

### *General Guidelines*

Follow these basic steps to configure OSPFv3:

1. Assign an IPv6 link-local address to each VLAN interface that will participate in an OSPF routing process. You can automatically generate a link-local address using the ipv6 enable command, or manually assign an address to an interface using the ipv6 address link-local command.

2. Use the router ipv6 ospf command to create a local OSPF router process and enter router configuration mode.

3. Use the router-id command to assign a unique identifier to the router. Note that the default router ID of “0.0.0.0” cannot be used with the current software version.

4. Use the ipv6 router ospf area command or the ipv6 router ospf tag area command to assign an area to each interface that will participate in the specified OSPF process.

## router ipv6 ospf

This command creates an Open Shortest Path First (OSPFv3) routing process and enters router configuration mode. Use the **no** form to disable OSPF for all processes or for a specified process.

### SYNTAX

[**no**] **router ipv6 ospf** [**tag** *process-name*]

*process-name* - A process name must be entered when configuring multiple routing instances. (Range: Alphanumeric string up to 16 characters)

### COMMAND MODE

Global Configuration

### DEFAULT SETTING

Disabled

### COMMAND USAGE

- This command is used to enable an OSPFv3 routing process, and to enter router configuration mode.

- The *process-name* is only used on the local router to distinguish between different routing processes. It should not be confused with the *instance-id* configured with the ipv6 router ospf area command which is used to distinguish between different routing processes running on the same link-local network segment.

### EXAMPLE

```
Console(config)#router ipv6 ospf tag 0
Console(config-router)#end
Console#show ipv6 ospf
 Routing Process "ospf r&d" with ID 192.168.0.2
 Process uptime is 1 hour 34 minutes
 Supports only single TOS(TOS0) routes
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Number of incoming concurrent DD exchange neighbors 0/5
 Number of outgoing concurrent DD exchange neighbors 0/5
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of LSA received 0
 Number of areas attached to this router: 1

    Area 0.0.0.0 (BACKBONE)
       SPF algorithm executed 1 times
       Number of LSA 2. Checksum 0x00ab4f

Console#
```

### RELATED COMMANDS

ipv6 router ospf area (1187)

## abr-type

This command sets the criteria used to determine if this router can declare itself an ABR and issue Type 3 and Type 4 summary LSAs. Use the **no** form to restore the default setting.

### SYNTAX

**abr-type** {**cisco** | **ibm** | **standard**}

**no abr-type**

**cisco** - ABR criteria and functional behavior is based on RFC 3509.

**ibm** - ABR criteria and functional behavior is briefly described in RFC 3509, and fully documented in IBM Nways Multiprotocol Routing Services (MRS) 3.3.

**standard** - ABR criteria and functional behavior is based on RFC 2328.

### COMMAND MODE

Router Configuration

### DEFAULT SETTING

cisco

### COMMAND USAGE

■The basic criteria for a router to serve as an ABR is shown below:

- Cisco Systems Interpretation: A router is considered to be an ABR if it has more than one area actively attached and one of them is the backbone area.
- IBM Interpretation: A router is considered to be an ABR if it has more than one actively attached area and the backbone area is configured.
- Standard Interpretation: A router is considered to be an ABR if it is attached to two or more areas. It does not have to be attached to the backbone area.

■To successfully route traffic to inter-area and AS external destinations, an ABR must be connected to the backbone. If an ABR has no backbone connection, all traffic destined for areas not connected to it or outside the AS will be dropped. This situation is normally resolved, by configuring a virtual link from the ABR to the backbone area.

■In both the Cisco and IBM interpretation, a router connected to more than one area cannot issue a Type 1 router LSA declaring itself as an ABR unless it meets the other criteria listed above.

Routing table calculations are changed to allow the router to consider summary-LSAs from all attached areas if it is not an ABR, but has more than one attached area, or it does not have an active backbone connection.

In other words, inter-area routes are calculated by examining summary-LSAs. If the router is an ABR and has an active backbone connection, only backbone summary-LSAs are examined. Otherwise (when either the router is not an ABR or it has no active backbone connection), the router should consider summary-LSAs from all actively attached areas.

This ensures that the summary-LSAs originated by area border routers advertise only intra-area routes into the backbone if the router has an active backbone connection, and advertises both intra-area and inter-area routes into the other areas. Otherwise, the router only advertises intra-area routes into non-backbone areas.

#### EXAMPLE

```
Console(config-router)#abr-type ibm
Console(config-router)#
```

## max-current-dd

This command sets the maximum number of neighbors with which the switch can concurrently exchange database descriptor (DD) packets. Use the **no** form to restore the default setting.

#### SYNTAX

**max-current-dd** *max-packets*

**no max-current-dd**

*max-packets* - The maximum number of neighbors with which the switch can concurrently send or receive DD packets. (Range: 1-65535)

#### COMMAND MODE
Router Configuration

#### DEFAULT SETTING
5

#### COMMAND USAGE
- This limit applies separately to the number of neighbors to which DD packets can be concurrently sent, and to the number of neighbors from which DD packets can be concurrently received.

#### EXAMPLE

```
Console(config-router)#maximum-current-dd 10
Console(config-router)#
```

#### RELATED COMMANDS
show ipv6 ospf (1194)

## router-id

This command assigns a unique router ID for this device within the autonomous system for the current OSPFv3 process. Use the **no** form to restore the default setting.

### SYNTAX

**router-id** *ip-address*

**no router-id**

*ip-address* - Router ID formatted as an IPv4 address.

### COMMAND MODE

Router Configuration

### DEFAULT SETTING

None

### COMMAND USAGE

- This command sets the router ID for the OSPF process specified in the router ipv6 ospf command.
- The router ID must be unique for every router in the autonomous system. (Note that the router ID can also be set to 255.255.255.255).
- If this router already has registered neighbors, the new router ID will be used when the router is rebooted, or manually restarted by entering the no router ipv6 ospf followed by the router ipv6 ospf command.
- If the priority values of the routers bidding to be the designated router or backup designated router for an area are equal, the router with the highest ID is elected.
- The current routing process will not be enabled until a Router ID is configured with this command.

### EXAMPLE

```
Console(config-router)#router-id 10.1.1.1
Console(config-router)#
```

### RELATED COMMANDS

router ipv6 ospf (1177)

## timers spf

This command configures the delay after receiving a topology change and starting the shortest path first (SPF) calculation, and the hold time between making two consecutive SPF calculations. Use the **no** form to restore the default values.

### SYNTAX

**timers spf** *spf-delay spf-holdtime*

**no timers spf**

*spf-delay* - The delay after receiving a topology change notification and starting the SPF calculation. (Range: 0-2147483647 seconds)

*spf-holdtime* - The minimum time between two consecutive SPF calculations. (Range: 0-2147483647 seconds)

### COMMAND MODE
Router Configuration

### DEFAULT SETTING
SPF delay: 5 seconds
SPF holdtime: 10 seconds

### COMMAND USAGE
- Setting the SPF holdtime to 0 means that there is no delay between consecutive calculations.

- Using a low value for the holdtime allows the router to switch to a new path faster, but uses more CPU processing time.

### EXAMPLE

```
Console(config-router)#timers spf 20
Console(config-router)#
```

## area default-cost

This command specifies a cost for the default summary route sent into a stub from an Area Border Router (ABR). Use the **no** form to remove the assigned default cost.

### SYNTAX

**area** *area-id* **default-cost** *cost*

**no area** *area-id* **default-cost**

*area-id* - Identifies the stub. (The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.)

*cost* - Cost for the default summary route sent to a stub. (Range: 0-16777215)

### COMMAND MODE
Router Configuration

### DEFAULT SETTING
Default cost: 1

### COMMAND USAGE
- If the default cost is set to "0," the router will not advertise a default route into the attached stub.

#### EXAMPLE

```
Console(config)#router ipv6 ospf tag 1
Console(config-router)#area 1 default-cost 1
Console(config-router)#
```

#### RELATED COMMANDS

area stub (1150)

### area range

This command summarizes the routes advertised by an Area Border Router (ABR). Use the **no** form to disable this function.

#### SYNTAX

[**no**] **area** *area-id* **range** *ipv6-prefix*/*prefix-length* {**advertise** | **not-advertise**}

*area-id* - Identifies an area for which the routes are summarized. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

*ipv6-prefix* - A full IPv6 address including the network prefix and host address bits.

*prefix-length* - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the portion of the address to summarize).

**advertise** - Advertises the specified address range.

**not-advertise** - The summary is not sent, and the routes remain hidden from the rest of the network.

#### COMMAND MODE

Router Configuration

#### DEFAULT SETTING

Disabled

#### COMMAND USAGE

- This command can be used to summarize intra-area routes and advertise this information to other areas through Area Border Routers (ABRs).

- If the network addresses within an area are assigned in a contiguous manner, the ABRs can advertise a summary route that covers all of the individual networks within the area that fall into the specified range using a single **area range** command.

- If routes are set to be advertised by this command, the router will issue a Type 3 summary LSA for each address range specified by this command.

- This router supports up 64 summary routes for area ranges.

### EXAMPLE

This example creates a summary address for all area routes in the range of 73::/8, or all IPv6 address that start with the first byte 73 (hexadecimal).

```
Console(config-router)#area 1 range 73::/8 advertise
Console(config-router)#
```

## default-metric

This command sets the default metric for external routes imported from other protocols. Use the **no** form to remove the default metric for the supported protocol types.

### SYNTAX

**default-metric** *metric-value*

**no default-metric**

*metric-value* – Metric assigned to all external routes imported from other protocols. (Range: 0-16777214)

### COMMAND MODE

Router Configuration

### DEFAULT SETTING

20

### COMMAND USAGE

- The default metric must be used to resolve the problem of redistributing external routes from other protocols that use incompatible metrics.
- This command does not override the metric value set by the redistribute command. When a metric value has not been configured by the redistribute command, the **default-metric** command sets the metric value to be used for all imported external routes.

### EXAMPLE

```
Console(config-router)#default-metric 100
Console(config-router)#
```

### RELATED COMMANDS

redistribute (1184)

## redistribute

This command redistributes external routing information from other routing protocols and static routes into an autonomous system. Use the **no** form to disable this feature or to restore the default settings.

### SYNTAX

**redistribute** {**connected** | **static**} [**metric** *metric-value*] [**metric-type** *type-value*]

**no redistribute** {**connected** | **rip** | **static**} [**metric**] [**metric-type**]

**connected** - Imports all currently connected entries.

**static** - IPv6 static routes will be imported into this Autonomous System.

*metric-value* - Metric assigned to all external routes for the specified protocol. (Range: 0-16777214: Default: 20)

*type-value*

**1** - Type 1 external route

**2** - Type 2 external route (default) - Routers do not add internal route metric to external route metric.

### COMMAND MODE

Router Configuration

### DEFAULT SETTING

redistribution - none
metric-value - 20
type-metric - 2

### COMMAND USAGE

- This command is used to import routes learned from other routing protocols into the OSPF domain, and to generate AS-external-LSAs.

- When you redistribute external routes into an OSPF autonomous system (AS), the router automatically becomes an autonomous system boundary router (ASBR).

- Metric type specifies the way to advertise routes to destinations outside the AS through External LSAs. When a Type 1 LSA is received by a router, it adds the internal cost to the external route metric. In other words, the cost of the route from any router within the AS is equal to the cost associated with reaching the advertising ASBR, plus the cost of the external route. When a Type 2 LSA is received by a router, it only uses the external route metric to determine route cost.

### EXAMPLE

This example redistributes automatically connected routes as Type 1 external routes.

```
Console(config-router)#redistribute connected metric-type 1
Console(config-router)#
```

## area stub

This command defines a stub area. To remove a stub, use the **no** form without the optional keyword. To remove the summary attribute, use the **no** form with the summary keyword.

### SYNTAX

[**no**] **area** *area-id* **stub** [**no-summary**]

*area-id* - Identifies the stub area. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

**no-summary** - Stops an Area Border Router (ABR) from sending summary link advertisements into the stub area.

### COMMAND MODE

Router Configuration

### DEFAULT SETTING

No stub is configured.
Summary advertisement are sent into the stub.

### COMMAND USAGE

- All routers in a stub must be configured with the same area ID.
- Routing table space is saved by stopping an ABR from flooding Type-4 Inter-Area Router and Type 5 AS-External LSAs into the stub. Since no information on external routes is known inside the stub, an ABR will advertise the default route 0::0/0 using a Type 3 Inter-Area Prefix LSA.
- The default setting for this command blocks Type-4 Inter-Area Router and Type 5 AS-External LSAs. Therefore, any destinations that cannot be matched to an inter-area or intra-area route will have to use the default route.
- Use the **no-summary** parameter of this command on an ABR attached to the stub to define a totally stubby area, blocking all Type 3 network summary LSAs. Define an area as a totally stubby area only if routers in the area do not require summary LSAs from other areas.
- Use the area default-cost command to specify the cost of a default summary route sent into a stub by an ABR attached to the stub area.

### EXAMPLE

This example creates a stub area 2, and makes it totally stubby by blocking all Type 3 summary LSAs.

```
Console(config-router)#area 2 stub no-summary
Console(config-router)#
```

### RELATED COMMANDS

area default-cost (1181)

## area virtual-link

This command defines a virtual link. To remove a virtual link, use the **no** form with no optional keywords. To restore the default value for an attribute, use the **no** form with the required keyword.vvvv

### Syntax

**area** *area-id* **virtual-link** *router-id*
[**dead-interval** *seconds*] [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*]

**no area area-id virtual-link** *router-id*
[**dead-interval | hello-interval | retransmit-interval | transmit-delay**]

*area-id* - Identifies the transit area for the virtual link.The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

*router-id* - Router ID of the virtual link neighbor. This specifies the Area Border Router (ABR) at the other end of the virtual link. To create a virtual link, enter this command for an ABR at both ends of the link. One of the ABRs must be next to the isolated area and the transit area at one end of the link, while the other ABR must be next to the transit area and backbone at the other end of the link.

**dead-interval** *seconds* - Specifies the time that neighbor routers will wait for a hello packet before they declare the router down. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 4 x hello interval, or 40 seconds)

**hello-interval** *seconds* - Specifies the transmit delay between sending hello packets. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase the routing traffic. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 10 seconds)

**retransmit-interval** *seconds* - Specifies the interval at which the ABR retransmits link-state advertisements (LSA) over the virtual link. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. However, note that this value should be larger for virtual links. (Range: 1-65535 seconds; Default: 5 seconds)

**transmit-delay** *seconds* - Estimates the time required to send a link-state update packet over the virtual link, considering the transmission and propagation delays. LSAs have their age incremented by this amount before transmission. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 1 second)

### Command Mode

Router Configuration

### Default Setting

*area-id*: None
*router-id*: None
**hello-interval**: 10 seconds
**retransmit-interval**: 5 seconds

**transmit-delay**: 1 second
**dead-interval**: 40 seconds

### COMMAND USAGE

- All areas must be connected to a backbone area (0.0.0.0) to maintain routing connectivity throughout the autonomous system. If it not possible to physically connect an area to the backbone, you can use a virtual link. A virtual link can provide a logical path to the backbone for an isolated area, or can be configured as a backup connection that can take over if the normal connection to the backbone fails.

- A virtual link can be configured between any two backbone routers that have an interface to a common non-backbone area. The two routers joined by a virtual link are treated as if they were connected by an unnumbered point-to-point network.

- Any area disconnected from the backbone must include the transit area ID and the router ID for a virtual link neighbor that is adjacent to the backbone.

### EXAMPLE

This example creates a virtual link using the defaults for all optional parameters.

```
Console(config-router)#area 3 virtual-link 192.168.0.9
Console(config-router)#
```

## ipv6 router ospf area

This command binds an OSPF area to the selected interface. Use the **no** form to remove an OSPF area, disable an OSPF process, or remove an instance identifier from an interface.

### SYNTAX

[**no**] **ipv6 router ospf area** *area-id* [**tag** *process-name* | **instance-id** *instance-id*]

*area-id* - Area to bind to the current Layer 3 interface. An OSPF area identifies a group of routers that share common routing information. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

*process-name* - A process name must be entered when configuring multiple routing instances. (Range: Alphanumeric string up to 16 characters)

*instance-id* - Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface. (Range: 0-255)

### COMMAND MODE

Interface Configuration

### DEFAULT SETTING

None

#### Command Usage

- An area ID uniquely defines an OSPF broadcast area. The area ID 0.0.0.0 indicates the OSPF backbone for an autonomous system. Each router must be connected to the backbone via a direct connection or a virtual link.
- Set the area ID to the same value for all routers on a network segment.
- The *process-name* is only used on the local router to distinguish between different routing processes (and must be configured with the router ipv6 ospf command before using it in the **ipv6 router ospf area** command).
- The *instance-id* is used on the link-local network segment to distinguish between different routing processes running on the same link, and allows routers participating in a common routing process to form adjacencies and exchange routing information.
- The backbone (area 0.0.0.0) must be created before any other area.

#### Example

This example creates the backbone 0.0.0.0.

```
Console(config)#router ipv6 ospf tag 0
Console(config-router)#router-id 192.168.0.2
Console(config-router)#exit
Console(config)#interface vlan 1
Console(config-if)#ipv6 router ospf area 0 tag 0 instance-id 0
Console(config-if)#
```

#### Related Commands

router ipv6 ospf (1177)
router-id (1180)
ipv6 router ospf tag area (1188)

### ipv6 router ospf tag area

This command binds an OSPF  area to the selected interface and process. Use the **no** form to remove the specified area from an interface.

[**no**] **ipv6 router ospf tag** *process-name* **area** *area-id* [**instance-id** *instance-id*]

*area-id* - Area to bind to the current Layer 3 interface. An OSPF area identifies a group of routers that share common routing information. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

*process-name* - A process name used to distinguish between multiple routing instances configured on the local router. (Range: Alphanumeric string up to 16 characters)

*instance-id* - Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface. (Range: 0-255)

#### Command Mode

Interface Configuration (VLAN)

**DEFAULT SETTING**

No areas are defined.

**COMMAND USAGE**

- An area ID uniquely defines an OSPF broadcast area. The area ID 0.0.0.0 indicates the OSPF backbone for an autonomous system. Each router must be connected to the backbone via a direct connection or a virtual link.
- Set the area ID to the same value for all routers on a network segment.
- The *process-name* is only used on the local router to distinguish between different routing processes (and must be configured with the router ipv6 ospf command before using it in this command.
- The *instance-id* is used on the link-local network segment to distinguish between different routing processes running on the same link, and allows routers participating in a common routing process to form adjacencies and exchange routing information.
- The backbone (area 0.0.0.0) must be created before any other area.

**EXAMPLE**

This example assigns area 0.0.0.1 to the currently selected interface under routing process "1."

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 router ospf tag 1 area 0.0.0.1
Console(config-if)#
```

**RELATED COMMANDS**

router ipv6 ospf (1177)
router-id (1180)
ipv6 router ospf area (1187)

## ipv6 ospf cost

This command explicitly sets the cost of sending a protocol packet on an interface, where higher values indicate slower ports. Use the **no** form to restore the default value.

**SYNTAX**

**ipv6 ospf cost** *cost* [**instance-id** *instance-id*]

**no ipv6 ospf cost** [**instance-id** *instance-id*]

*cost* - Link metric for this interface. Use higher values to indicate slower ports. (Range: 1-65535)

*instance-id* - Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface. (Range: 0-255)

**COMMAND MODE**

Interface Configuration (VLAN)

### DEFAULT SETTING

1

### COMMAND USAGE

- The interface cost indicates the overhead required to send packets across a certain interface. This is advertised as the link cost in router link state advertisements.
- Routes are assigned a metric equal to the sum of all metrics for each interface link in the route.
- This router uses a default cost of 1 for all interfaces. Therefore, if you install a 10 Gigabit module, you may need to reset the cost for all other VLAN interfaces with only 1 Gbps ports to a value greater than 1 to reflect the actual interface bandwidth.

### EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 ospf cost 10
Console(config-if)#
```

## ipv6 ospf dead-interval

This command sets the interval at which hello packets are not seen before neighbors declare the router down. Use the **no** form to restore the default value.

### SYNTAX

**ipv6 ospf dead-interval** *seconds* [**instance-id** *instance-id*]

**no ipv6 ospf dead-interval** [**instance-id** *instance-id*]

*seconds* - The maximum time that neighbor routers can wait for a hello packet before declaring the transmitting router down. This interval must be set to the same value for all routers on the network. (Range: 1-65535)

*instance-id* - Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface. (Range: 0-255)

### COMMAND MODE

Interface Configuration (VLAN)

### DEFAULT SETTING

40 seconds, or four times the interval specified by the ipv6 ospf hello-interval command.

### COMMAND USAGE

The dead-interval is advertised in the router's hello packets. It must be a multiple of the hello-interval and be the same for all routers on a specific network.

### EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 ospf dead-interval 50
Console(config-if)#
```

### RELATED COMMANDS

ipv6 ospf hello-interval (1191)

## ipv6 ospf hello-interval

This command specifies the interval between sending hello packets on an interface. Use the **no** form to restore the default value.

### SYNTAX

**ipv6 ospf hello-interval** *seconds* [**instance-id** *instance-id*]

**no ipv6 ospf hello-interval** [**instance-id** *instance-id*]

*seconds* - Interval at which hello packets are sent from an interface. This interval must be set to the same value for all routers on the network. (Range: 1-65535)

*instance-id* - Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface. (Range: 0-255)

### COMMAND MODE

Interface Configuration (VLAN)

### DEFAULT SETTING

10 seconds

### COMMAND USAGE

Hello packets are used to inform other routers that the sending router is still active. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase routing traffic.

### EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 ospf hello-interval 5
Console(config-if)#
```

### RELATED COMMANDS

ipv6 ospf dead-interval (1190)

## ipv6 ospf priority

This command sets the router priority used when determining the designated router (DR) and backup designated router (BDR) for an area. Use the **no** form to restore the default value.

### SYNTAX

**ipv6 ospf priority** *priority* [**instance-id** *instance-id*]

**no ipv6 ospf priority** [**instance-id** *instance-id*]

*priority* - Sets the interface priority for this router. (Range: 0-255)

*instance-id* - Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface. (Range: 0-255)

### Command Mode
Interface Configuration (VLAN)

### Default Setting
1

### Command Usage
- A designated router (DR) and backup designated router (BDR) are elected for each OSPF area based on Router Priority. The DR forms an active adjacency to all other routers in the area to exchange routing topology information. If for any reason the DR fails, the BDR takes over this role.
- Set the priority to zero to prevent a router from being elected as a DR or BDR. If set to any value other than zero, the router with the highest priority will become the DR and the router with the next highest priority becomes the BDR. If two or more routers are tied with the same highest priority, the router with the higher ID will be elected.
- If a DR already exists for a network segment when this interface comes up, the new router will accept the current DR regardless of its own priority. The DR will not change until the next time the election process is initiated.
- Configure router priority for multi-access networks only and not for point-to-point networks.

### Example
```
Console(config)#interface vlan 1
Console(config-if)#ipv6 ospf priority 5
Console(config-if)#
```

## ipv6 ospf retransmit-interval

This command specifies the time between resending link-state advertisements (LSAs). Use the **no** form to restore the default value.

### Syntax

**ipv6 ospf retransmit-interval** *seconds* [**instance-id** *instance-id*]

**no ipv6 ospf retransmit-interval** [**instance-id** *instance-id*]

*seconds* - Sets the interval at which LSAs are retransmitted from this interface. (Range: 1-65535)

*instance-id* - Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface. (Range: 0-255)

### COMMAND MODE

Interface Configuration (VLAN)

### DEFAULT SETTING

5 seconds

### COMMAND USAGE

- A router will resend an LSA to a neighbor if it receives no acknowledgment after the specified retransmit interval. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. Note that this value should be larger for virtual links.

- Set this interval to a value that is greater than the round-trip delay between any two routers on the attached network to avoid unnecessary retransmissions.

### EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 ospf retransmit-interval 7
Console(config-if)#
```

## ipv6 ospf transmit-delay

This command sets the estimated time to send a link-state update packet over an interface. Use the **no** form to restore the default value.

### SYNTAX

**ipv6 ospf transmit-delay** *seconds* [**instance-id** *instance-id*]

**no ipv6 ospf transmit-delay** [**instance-id** *instance-id*]

*seconds* - Sets the estimated time required to send a link-state update. (Range: 1-65535)

*instance-id* - Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface. (Range: 0-255)

### COMMAND MODE

Interface Configuration (VLAN)

### DEFAULT SETTING

1 second

### COMMAND USAGE

- LSAs have their age incremented by this delay before transmission. When estimating the transmit delay, consider both the transmission and propagation delays for an interface. Set the transmit delay according to link speed, using larger values for lower-speed links.

- If this delay is not added, the time required to transmit an LSA over the link is not taken into consideration by the routing process. On slow links, the router may send packets more quickly than devices can receive them. To avoid this problem, use the transmit delay to force the router to wait a specified interval between transmissions.

### Example

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 ospf transmit-delay 6
Console(config-if)#
```

## passive-interface

This command suppresses OSPF routing traffic on the specified interface. Use the **no** form to allow routing traffic to be sent and received on the specified interface.

### Syntax

[**no**] **passive-interface vlan** *vlan-id* [*ipv6-address*]

*vlan-id* - VLAN ID. (Range: 1-4093)

*ipv6-address* - A full IPv6 address including the network prefix and host address bits.

### Command Mode

Router Configuration

### Default Setting

None

### Command Usage

You can configure an OSPF interface as passive to prevent OSPF routing traffic from exiting or entering that interface. No OSPF adjacency can be formed if one of the interfaces involved is set to passive mode. The specified interface will appear as a stub in the OSPF domain. Also, if you configure an OSPF interface as passive where an adjacency already exists, the adjacency will drop almost immediately.

### Example

```
Console(config-router)#passive-interface vlan 1 73::9
Console(config-router)#
```

## show ipv6 ospf

This command shows basic information about the routing configuration.

### Command Mode

Privileged Exec

### Example

```
Console#show ipv6 ospf
  Routing Process "ospf 1" with ID 192.168.0.2
 Process uptime is 24 minutes
 Supports only single TOS(TOS0) routes
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Number of incoming concurrent DD exchange neighbors 0/5
```

```
Number of outgoing concurrent DD exchange neighbors 0/5
Number of external LSA 0. Checksum 0x000000
Number of opaque AS LSA 0. Checksum 0x000000
Number of LSA received 0
Number of areas attached to this router: 2

  Area 0.0.0.0 (BACKBONE)
    SPF algorithm executed 2 times
    Number of LSA 1. Checksum 0x001aa9
  Area 0.0.0.1
    SPF algorithm executed 2 times
    Number of LSA 1. Checksum 0x001aa9

Console#
```

**Table 17: show ip ospf** - display description

| Field | Description |
| --- | --- |
| *Routing Process* | |
| Routing Process | OSPF process name and router ID. The router ID uniquely identifies the router in the autonomous system. By convention, this is normally set to one of the router's IP interface addresses. |
| Process uptime | The time this process has been running |
| Supports only single TOS (TOS0) routes | Optional Type of Service (ToS) specified in OSPF Version 2, Appendix F.1.2 is not supported, so only one cost per interface can be assigned. |
| SPF schedule delay | The delay after receiving a topology change notification and starting the SPF calculation. |
| Hold time | Sets the hold time between two consecutive SPF calculations. |
| Number of concurrent DD exchange neighbors | Number of neighbors currently exchanging database descriptor packets. |
| Number of external LSA | The number of external link-state advertisements (Type 5 LSAs) in the link-state database. These LSAs advertise information about routes outside of the autonomous system. |
| Checksum | The sum of the LS checksums of the external link-state advertisements contained in the link-state database. |
| Number of opaque AS LSA | Number of opaque link-state advertisements (Type 9, 10 and 11 LSAs) in the link-state database. These LSAs advertise information about external applications, and are only used by OSPF for the graceful restart process. |
| Checksum | The sum of the LS checksums of opaque link-state advertisements contained in the link-state database. |
| Number of LSA received | The number of link-state advertisements that have been received. |
| Number of areas attached to this router | The number of configured areas attached to this router. |
| *Area Information* | |
| Area | The area identifier. Note that “(Inactive)” will be displayed if no IPv6 address has been configured on the interface. |
| SPF algorithm executed x times | The number of times the shortest path first algorithm has been executed for this area |

**Table 17: show ip ospf** - display description (Continued)

| Field | Description |
|---|---|
| Number of LSA | The total number of link-state advertisements in this area's link-state database, excluding AS External LSA's. |
| Checksum | The sum of the LS checksums of link-state advertisements for this network (area) contained in the link-state database. |

## show ipv6 ospf database

This command shows information about different OSPF Link State Advertisements (LSAs) stored in this router's database.

### Syntax

**show ipv6 ospf** [**tag** *process-id*] **database**

*process-id* - The ID of the router process for which information will be displayed. (Range: 1-10)

### Command Mode

Privileged Exec

### Examples

The following shows output for the **show ip ospf database** command.

```
Console#show ipv6 ospf database

            OSPF Router with ID (192.168.0.2) (TAG: 1)

                Link-LSA
Link State ID   ADV Router     Age  Seq#      CkSum    Link
1001            192.168.0.2     71 0x80000001 0x06b7    0

                Router-LSA (Area 0)
Link State ID   ADV Router     Age  Seq#      CkSum
0               192.168.0.2     31 0x80000002 0x14b1

                AS-external-LSA
Link State ID   ADV Router     Age  Seq#      CkSum
Console#
```

**Table 18: show ip ospf database** - display description

| Field | Description |
|---|---|
| OSPF Router Process with ID | OSPF router ID and process ID. The router ID uniquely identifies the router in the autonomous system. By convention, this is normally set to one of the router's IP interface addresses. |
| Link State ID | This field identifies the piece of the routing domain that is being described by the advertisement. |
| ADV Router | Advertising router ID |
| Age | Age of LSA (in seconds) |
| Seq# | Sequence number of LSA (used to detect older duplicate LSAs) |

**Table 18: show ip ospf database** - display description (Continued)

| Field | Description |
|---|---|
| CkSum | Checksum of the complete contents of the LSA |
| Link | Number of interfaces attached to the router |

## show ipv6 ospf interface

This command displays summary information for OSPF interfaces.

### SYNTAX

**show ipv6 ospf interface** [**vlan** *vlan-id*]

*vlan-id* - VLAN ID (Range: 1-4093)

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show ipv6 ospf interface vlan 1
 VLAN 1 is up, line protocol is up
 Link local Address FE80::200:E8FF:FE93:82A0/64, Area 0.0.0.0
 Tag 1, Router ID 192.168.0.2, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State DR, Priority 1
 Designated Router (ID) 192.168.0.2, Interface Address FE80::200:E8FF:FE93:82A0
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Neighbor Count is 0, Adjacent neighbor count is 0
 Hello received 0 sent 92, DD received 0 sent 0
 LS-Req received 0 sent 0, LS-Upd received 0 sent 0
 LS-Ack received 0 sent 0, Discarded 0
Console#
```

**Table 19: show ip ospf interface** - display description

| Field | Description |
|---|---|
| VLAN | VLAN ID and Status of physical link |
| Link local Address | Link local address of OSPF interface |
| Area | OSPF area to which this interface belongs |
| Tag | OSPF process identifier string |
| Router ID | Identifier for this router |
| Network Type | Includes broadcast, non-broadcast, or point-to-point networks |
| Cost | Interface transmit cost |
| Transmit Delay | Interface transmit delay (in seconds) |

**Table 19: show ip ospf interface** - display description (Continued)

| Field | Description |
|---|---|
| State | ◆ Backup – Backup Designated Router<br>◆ Down – OSPF is enabled on this interface, but interface is down<br>◆ DR – Designated Router<br>◆ DROther – Interface is on a multiaccess network, but is not the DR or BDR<br>◆ Loopback – This is a loopback interface<br>◆ PointToPoint – A direct link between two routers.<br>◆ Waiting – Router is trying to find the DR and BDR |
| Priority | Router priority |
| Designated Router | Designated router ID and respective interface address |
| Backup Designated Router | Backup designated router ID and respective interface address |
| Timer intervals | Configuration settings for timer intervals, including Hello, Dead and Retransmit |
| Neighbor Count | Count of network neighbors and adjacent neighbors |
| Hello | Number of Hello LSAs received and sent |
| DD | Number of Database Descriptor packets received and sent |
| LS-Req | Number of LSA requests |
| LS-Upd | Number of LSA updates |
| LS-Ack | Number of LSA acknowledgements |
| Discarded | Number of LSAs discarded |

## show ipv6 ospf neighbor

This command displays information about neighboring routers on each interface within an OSPF area.

### Syntax

**show ipv6 ospf** [**tag** *process-id*] **neighbor**

*process-id* - The ID of the router process for which information will be displayed. (Range: 1-10)

### Command Mode

Privileged Exec

### Example

```
Console#show ipv6 ospf neighbor

      ID        Pri     State      Interface ID   Interface
--------------- ------ ---------------- --------------- --------------
```

```
  192.168.0.2    1       FULL/DR         1001    vlan1
Console#
```

**Table 20: show ipv6 ospf neighbor** - display description

| Field | Description |
|---|---|
| ID | Neighbor’s router ID |
| Pri | Neighbor’s router priority |
| State | OSPF state and identification flag<br>States include:<br>Down – Connection down<br>Attempt – Connection down, but attempting contact (for non-broadcast networks)<br>Init – Have received Hello packet, but communications not yet established<br>Two-way – Bidirectional communications established<br>ExStart – Initializing adjacency between neighbors<br>Exchange – Database descriptions being exchanged<br>Loading – LSA databases being exchanged<br>Full – Neighboring routers now fully adjacent<br><br>Identification flags include:<br>D – Dynamic neighbor<br>S – Static neighbor<br>DR – Designated router<br>BDR – Backup designated router |
| Interface ID | |
| Interface | The interface to which this neighbor is attached |

## show ipv6 ospf route

This command displays the OSPF routing table.

### SYNTAX

**show ipv6 ospf** [**tag** *process-id*] **route**

*process-id* - The ID of the router process for which information will be displayed. (Range: 1-10)

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show ipv6 ospf route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
C    ::1/128, lo0
O    2001:DB8:2222:7272::/64, VLAN1
C    2001:DB8:2222:7272::/64, VLAN1
?    FE80::/64, VLAN1 inactive
C    FE80::/64, VLAN1
?    FF00::/8, VLAN1 inactive

Console#
```

## show ipv6 ospf virtual-links

This command displays detailed information about virtual links.

### SYNTAX

**show ipv6 ospf** [**tag** *process-id*] **virtual-links**

*process-id* - The ID of the router process for which information will be displayed. (Range: 1-10)

### COMMAND MODE

Privileged Exec

### EXAMPLE

```
Console#show ip ospf virtual-links
Virtual Link VLINK1 to router 192.168.0.2 is up
  Transit area 0.0.0.1 via interface vlan1
  Local address 192.168.0.3
  Remote address 192.168.0.2
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
    Adjacency state Full
Console#
```

**Table 21: show ip ospf neighbor** - display description

| Field | Description |
|---|---|
| Virtual Link to router | OSPF neighbor and link state (up or down) |
| Transit area | Common area the virtual link crosses to reach the target router |
| Local address | The IP address of ABR that serves as an endpoint connecting the isolated area to the common transit area. |
| Remote address | The IP address this virtual neighbor is using. The neighbor must be an ABR at the other endpoint connecting the common transit area to the backbone itself. |
| Transmit Delay | Estimated transmit delay (in seconds) on the virtual link |
| Timer intervals | Configuration settings for timer intervals, including Hello, Dead and Retransmit |
| Hello due | The timeout for the next hello message from the neighbor |
| Adjacency state | The adjacency state between these neighbors:<br>Down – Connection down<br>Attempt – Connection down, but attempting contact (for non-broadcast networks)<br>Init – Have received Hello packet, but communications not yet established<br>Two-way – Bidirectional communications established<br>ExStart – Initializing adjacency between neighbors<br>Exchange – Database descriptions being exchanged<br>Loading – LSA databases being exchanged<br>Full – Neighboring routers now fully adjacent |

### RELATED COMMANDS

area virtual-link (1186)

# 49 MULTICAST ROUTING COMMANDS

Multicast routers can use various kinds of multicast routing protocols to deliver IP multicast packets across different subnetworks. This router supports Protocol Independent Multicasting (PIM). (Note that IGMP will be enabled for any interface that is using multicast routing.)

**Table 1: Multicast Routing Commands**

| Command Group | Function |
|---|---|
| General Multicast Routing | Enables IP multicast routing globally; also displays the IP multicast routing table created from static and dynamic routing information |
| Static Multicast Routing | Configures static multicast router ports |
| PIM Multicast Routing | Configures global and interface settings for PIM-DM and PIM-SM |

## GENERAL MULTICAST ROUTING

This section describes commands used to configure multicast routing globally on the switch.

**Table 2: General Multicast Routing Commands**

| Command | Function | Mode |
|---|---|---|
| IPv4 Commands | | |
| ip multicast-routing | Enables IPv4 multicast routing | GC |
| show ip mroute | Shows the IPv4 multicast routing table | PE |
| IPv6 Commands | | |
| ipv6 multicast-routing | Enables IPv6 multicast routing | GC |
| show ipv6 mroute | Shows the IPv6 multicast routing table | PE |

### ip multicast-routing

This command enables IPv4 multicast routing. Use the **no** form to disable IP multicast routing.

#### SYNTAX

[**no**] **ip multicast-routing**

#### DEFAULT SETTING

Disabled

#### COMMAND MODE

Global Configuration

### COMMAND USAGE

- This command is used to enable IPv4 multicast routing globally for the router. A specific multicast routing protocol also needs to be enabled on the interfaces that will support multicast routing using the router pim command, and then specify the interfaces that will support multicast routing using the ip pim dense-mode or ip pim sparse-mode commands.

- To use multicast routing, IGMP proxy can not enabled on any interface of the device (see ip igmp proxy on page 1001).

### EXAMPLE

```
Console(config)#ip multicast-routing
Console(config)#
```

## show ip mroute

This command displays the IPv4 multicast routing table.

### SYNTAX

**show ip mroute** [*group-address source*] [**summary**]

*group-address* - An IPv4 multicast group address with subscribers directly attached or downstream from this router.

*source* - The IPv4 subnetwork at the root of the multicast delivery tree. This subnetwork contains a known multicast source.

**summary** - Displays summary information for each entry in the IP multicast routing table.

### COMMAND MODE

Privileged Exec

### COMMAND USAGE

This command displays information for multicast routing. If no optional parameters are selected, detailed information for each entry in the multicast address table is displayed. If you select a multicast group and source pair, detailed information is displayed only for the specified entry. If the **summary** option is selected, an abbreviated list of information for each entry is displayed on a single line.

### EXAMPLE

This example shows detailed multicast information for a specified group/source pair

```
Console#show ip mroute 224.0.255.3 192.111.46.8

IP Multicast Forwarding is enabled.

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, s - SSM Channel, C - Connected, P - Pruned,
      F - Register flag, R - RPT-bit set, T - SPT-bit set, J - Join SPT
Interface state: F - Forwarding, P - Pruned, L - Local

(192.168.2.1, 224.0.17.17), uptime 00:00:05
Owner: PIM-DM, Flags: D
```

```
Incoming Interface: VLAN2, RPF neighbor: 192.168.2.1
Outgoing Interface List:
VLAN1(F)

Console#
```

**Table 3: show ip mroute** - display description

| Field | Description |
|---|---|
| Flags | The flags associated with this entry:<br>◆ D (Dense) - PIM Dense mode in use.<br>◆ S (Sparse) - PIM Sparse mode in use.<br>◆ s (SSM) - A multicast group with the range of IP addresses used for PIM-SSM.<br>◆ C (Connected) - A member of the multicast group is present on this interface.<br>◆ P (Pruned) - This route has been terminated.<br>◆ F (Register flag) - This device is registering for a multicast source.<br>◆ R (RP-bit set) - The (S,G) entry is pointing to the Rendezvous Point (RP), which normally indicates a pruned state along the shared tree for a particular source.<br>◆ T (SPT-bit set) - Multicast packets have been received from a source on the shortest path tree.<br>◆ J (Join SPT) - The rate of traffic arriving over the shared tree has exceeded the SPT-threshold for this group. If the SPT flag is set for (*,G) entries, the next (S,G) packet received will cause the router to join the shortest path tree. If the SPT flag is set for (S,G), the router immediately joins the shortest path tree. |
| Interface state | The multicast state for the displayed interface. |
| group address | IP multicast group address for a requested service. |
| source | Subnetwork containing the IP multicast source. |
| uptime | The time elapsed since this entry was created. |
| Owner | The associated multicast protocol (PIM). |
| Incoming Interface | Interface leading to the upstream neighbor.<br>PIM creates a multicast routing tree based on the unicast routing table. If the related unicast routing table does not exist, PIM will still create a multicast routing entry, but displays “Null” for the upstream interface to indicate that the unicast routing table is not valid. This field may also display “Register” to indicate that a pseudo interface is being used to send or receive PIM-SM register packets. |
| RPF neighbor | IP address of the multicast router immediately upstream for this group. |
| Outgoing interface list and flags | The interface(s) on which multicast subscribers have been recorded. The flags associated with each interface indicate:<br>◆ F (Register flag) - This device is registering for a multicast source.<br>◆ P (Pruned) - This route has been terminated.<br>◆ L (Local) - Downstream interface has received IGMP report message from host in this subnet. |

This example lists all entries in the multicast table in summary form:

```
Console#show ip mroute summary

IP Multicast Forwarding is enabled
```

```
IP Multicast Routing Table (Summary)
Flags: F – Forwarding,  P - Pruned
    Group          Source        Source Mask    Interface  Owner   Flags
--------------- --------------- --------------- ---------- ------- ------
   224.0.17.17     192.168.2.1 255.255.255.255 VLAN2      PIM-DM  F
 Total Entry is 1

Console#
```

## ipv6 multicast-routing

This command enables IPv6 multicast routing. Use the **no** form to disable IP multicast routing.

### SYNTAX

[**no**] **iv6p multicast-routing**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- This command is used to enable IPv6 multicast routing globally for the router. A multicast routing protocol also needs to be enabled on the interfaces that will support multicast routing using the router pim6 command, and then specify the interfaces that will support multicast routing using the ipv6 pim dense-mode command.

- To use multicast routing, MLD proxy can not enabled on any interface of the device (see ipv6 mld proxy on page 1011).

### EXAMPLE

```
Console(config)#ipv6 multicast-routing
Console(config)#
```

## show ipv6 mroute

This command displays the IPv6 multicast routing table.

### SYNTAX

**show ipv6 mroute** [*group-address source*] [**summary**]

*group-address* - An IPv6 multicast group address with subscribers directly attached or downstream from this router.

*source* - The IPv6 subnetwork at the root of the multicast delivery tree. This subnetwork contains a known multicast source.

**summary** - Displays summary information for each entry in the IP multicast routing table.

### COMMAND MODE

Privileged Exec

### COMMAND USAGE

This command displays information for multicast routing. If no optional parameters are selected, detailed information for each entry in the multicast address table is displayed. If you select a multicast group and source pair, detailed information is displayed only for the specified entry. If the **summary** option is selected, an abbreviated list of information for each entry is displayed on a single line.

### EXAMPLE

This example shows detailed multicast information for a specified group/source pair

```
Console#show ipv6 mroute FF02::0101 FE80::0202

IP Multicast Forwarding is enabled.

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, s - SSM Channel, C - Connected, P - Pruned,
      F - Register flag, R - RPT-bit set, T - SPT-bit set, J - Join SPT
Interface state: F - Forwarding, P - Pruned, L - Local

(FF02::0101, FE80::0202), uptime 00:00:05
Owner: PIM-DM, Flags: D
Incoming Interface: VLAN2, RPF neighbor: FE80::0303
Outgoing Interface List:
VLAN1(F)
Console#
```

**Table 4: show ip mroute** - display description

| Field | Description |
|---|---|
| Flags | The flags associated with this entry:<br>◆D (Dense) - PIM Dense mode in use.<br>◆S (Sparse) - PIM Sparse mode in use.<br>◆s (SSM) - A multicast group with the range of IP addresses used for PIM-SSM.<br>◆C (Connected) - A member of the multicast group is present on this interface.<br>◆P (Pruned) - This route has been terminated.<br>◆F (Register flag) - This device is registering for a multicast source.<br>◆R (RP-bit set) - The (S,G) entry is pointing to the Rendezvous Point (RP), which normally indicates a pruned state along the shared tree for a particular source.<br>◆T (SPT-bit set) - Multicast packets have been received from a source on the shortest path tree.<br>◆J (Join SPT) - The rate of traffic arriving over the shared tree has exceeded the SPT-threshold for this group. If the SPT flag is set for (*,G) entries, the next (S,G) packet received will cause the router to join the shortest path tree. If the SPT flag is set for (S,G), the router immediately joins the shortest path tree. |
| Interface state | The multicast state for the displayed interface. |
| group address | IP multicast group address for a requested service. |
| source | Subnetwork containing the IP multicast source. |

**Table 4: show ip mroute** - display description

| Field | Description |
|---|---|
| Uptime | The time elapsed since this entry was created. |
| Owner | The associated multicast protocol (PIM). |
| Incoming Interface | Interface leading to the upstream neighbor.<br>PIM creates a multicast routing tree based on the unicast routing table. If the related unicast routing table does not exist, PIM will still create a multicast routing entry, but displays “Null” for the upstream interface to indicate that the unicast routing table is not valid. This field may also display “Register” to indicate that a pseudo interface is being used to send or receive PIM-SM register packets. |
| RPF neighbor | IP address of the multicast router immediately upstream for this group. |
| Outgoing interface list and flags | The interface(s) on which multicast subscribers have been recorded. The flags associated with each interface indicate:<br>◆F (Register flag) - This device is registering for a multicast source.<br>◆P (Pruned) - This route has been terminated.<br>◆L (Local) - Downstream interface has received IGMP report message from host in this subnet. |

This example lists all entries in the multicast table in summary form:

```
Console#show ipv6 mroute summary

IP Multicast Forwarding is disabled

IP Multicast Routing Table (Summary)
Flags:  F - Forwarding, P - Pruned, D - PIM-DM, S – PIM-SM, V – DVMRP,
       M - MLD
Group                         Source                        Interface  Flag
----------------------------- ----------------------------- ---------- ----
           FF02::0101                FE80::0101 VLAN 4096   DF
Total Entry is 1
Console#
```

## STATIC MULTICAST ROUTING

This section describes commands used to configure static multicast routes on the switch.

**Table 5: Static Multicast Routing Commands**

| Command | Function | Mode |
|---|---|---|
| ip igmp snooping vlan mrouter | Adds a multicast router port | GC |
| show ip igmp snooping mrouter | Shows multicast router ports | PE |

### ip igmp snooping vlan mrouter

This command statically configures a multicast router port. Use the **no** form to remove the configuration.

#### SYNTAX

**ip igmp snooping vlan** *vlan-id* **mrouter** *interface*

**no ip igmp snooping vlan** *vlan-id* **mrouter** *interface*

*vlan-id* - VLAN ID (Range: 1-4093)

*interface*

**ethernet** *unit*/*port*

*port* - Port number. (Range: 1-12/14/16/18) depending on the model

**port-channel** *channel-id* (Range: 1-32)

#### 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: 1-4093)

#### DEFAULT SETTING
Displays multicast router ports for all configured VLANs.

#### COMMAND MODE
Privileged Exec

#### COMMAND USAGE
Multicast router port types displayed include Static or Dynamic.

#### 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  Dynamic
Console#
```

## PIM MULTICAST ROUTING

This section describes the PIM commands used for IPv4 and IPv6. Note that PIM can run on an IPv4 network and PIM6 on an IPv6 network simultaneously. Also note that Internet Group Management Protocol (IGMP) is used for IPv4 networks and Multicast Listener Discovery (MLD) for IPv6 networks.

**Table 6: IPv4 and IPv6 PIM Commands**

| Command Group | Function |
|---|---|
| IPv4 PIM Commands | Configures multicast routing for IPv4 PIM. |
| IPv6 PIM Commands | Co figures multicast routing for IPv6 PIM. |

### IPV4 PIM COMMANDS

This section describes commands used to configure IPv4 PIM-DM and PIM-SM dynamic multicast routing on the switch.

**Table 7: PIM-DM and PIM-SM Multicast Routing Commands**

| Command | Function | Mode |
|---|---|---|
| Common Commands | | |
| router pim | Enables IPv4 PIM globally for the router | GC |
| ip pim | Enables PIM-DM or PIM-SM on the specified interface | IC |
| ip pim hello-holdtime | Sets the time to wait for hello messages from a neighboring PIM router before declaring it dead | IC |
| ip pim hello-interval | Sets the interval between sending PIM hello messages | IC |
| ip pim join-prune-holdtime | Configures the hold time for the prune state | IC |
| ip pim lan-prune-delay | Informs downstream routers of the delay before it prunes a flow after receiving a prune request | IC |
| ip pim override-interval | Specifies the time it takes a downstream router to respond to a lan-prune-delay message | IC |
| ip pim propagation-delay | Configures the propagation delay required for a LAN prune delay message to reach downstream routers | IC |
| ip pim trigger-hello-delay | Configures the trigger hello delay | IC |
| show ip pim interface | Displays information about interfaces configured for PIM | NE, PE |
| show ip pim neighbor | Displays information about PIM neighbors | NE, PE |

**Table 7: PIM-DM and PIM-SM Multicast Routing Commands (Continued)**

| Command | Function | Mode |
|---|---|---|
| PIM-DM Commands | | |
| ip pim graft-retry-interval | Configures the time to wait for a Graft acknowledgement before resending a Graft message | IC |
| ip pim max-graft-retries | Configures the maximum number of times to resend a Graft message if it has not been acknowledged | IC |
| ip pim state-refresh origination-interval | Sets the interval between PIM-DM state refresh control messages | IC |
| PIM-SM Commands | | |
| ip pim bsr-candidate | Configures the switch as a Bootstrap Router (BSR) candidate | GC |
| ip pim register-rate-limit | Configures the rate at which register messages are sent by the Designated Router (DR) | GC |
| ip pim register-source | Configure the IP source address of a register message to an address other than the outgoing interface address of the designated router (DR) leading toward the rendezvous point (RP) | GC |
| ip pim rp-address | Sets a static address for the rendezvous point | GC |
| ip pim rp-candidate | Configures the switch rendezvous point (RP) candidate | GC |
| ip pim spt-threshold | Prevents the last-hop PIM router from switching to Shortest Path Source Tree (SPT) mode | GC |
| ip pim dr-priority | Sets the priority value for a DR candidate | IC |
| ip pim join-prune-interval | Sets the join/prune timer | IC |
| clear ip pim bsr rp-set | Clears RP entries learned through the BSR | PE |
| show ip pim bsr-router | Displays information about the BSR | PE |
| show ip pim rp mapping | Displays active RPs and associated multicast routing entries | PE |
| show ip pim rp-hash | Displays the RP used for the specified multicast group | PE |

## router pim

This command enables IPv4 Protocol-Independent Multicast routing globally on the router. Use the **no** form to disable PIM multicast routing.

### SYNTAX

[**no**] **router pim**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- This command enables PIM-DM and PIM-SM globally for the router. You also need to enable PIM-DM or PIM-SM for each interface that will support multicast routing using the ip pim dense-mode or ip pim sparse mode command, and make any changes necessary to the multicast protocol parameters.

- To use multicast routing, IGMP proxy can not enabled on any interface of the device (see the ip igmp proxy command).

### EXAMPLE

```
Console(config)#router pim
Console(config)#exit
Console#show ip pim interface
PIM is enabled.
Vlan 1 is up.
 PIM Mode               :    Dense Mode
 IP Address             :    192.168.0.2
 Hello Interval         :    30 sec
 Hello HoldTime         :    105 sec
 Triggered Hello Delay  :    5 sec
 Join/Prune Holdtime    :    210 sec
 Lan Prune Delay        :    Disabled
 Propagation Delay      :    500  ms
 Override Interval      :    2500  ms
 Graft Retry Interval   :    3 sec
 Max Graft Retries      :    3
 State Refresh Ori Int  :    60 sec

Console#
```

## ip pim

This command enables PIM-DM on the specified interface. Use the **no** form to disable PIM-DM on this interface.

### SYNTAX

[**no**] **ip pim** {**dense-mode** | **sparse-mode**}

**dense-mode** - Enables PIM Dense Mode.

**sparse-mode -** Enables PIM Sparse Mode.

### DEFAULT SETTING

Disabled

### COMMAND MODE

Interface Configuration (VLAN)

### COMMAND USAGE

- To fully enable PIM, you need to enable multicast routing globally for the router with the ip multicast-routing command, enable PIM globally for the router with the router pim command, and also enable PIM-DM or PIM-SM for each interface that will participate in multicast routing with this command.

- If you enable PIM on an interface, you should also enable IGMP on that interface. PIM mode selection determines how the switch populates the multicast routing table, and how it forwards packets received from directly connected LAN interfaces.Dense mode interfaces are always added to the multicast routing table. Sparse mode interfaces are added only when periodic join messages are received from downstream routers, or a group member is directly connected to the interface.

- Dense-mode interfaces are subject to multicast flooding by default, and are only removed from the multicast routing table when the router determines that there are no group members or downstream routers, or when a prune message is received from a downstream router.
- Sparse-mode interfaces forward multicast traffic only if a join message is received from a downstream router or if group members are directly connected to the interface. When routers want to receive a multicast flow, they periodically send join messages to the Rendezvous Point (RP), and are subsequently added to the shared path for the specified flow back up to the RP. If routers want to join the source path up through the Shortest Path Source Tree (SPT), they periodically send join messages toward the source. They also send prune messages toward the RP to prune the shared path if they have already connected to the source through the SPT, or if there are no longer any group members connected to the interface.

### EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip pim dense-mode
Console#show ip pim interface
PIM is enabled.
Vlan 1 is up.
 PIM Mode              :     Dense Mode
 IP Address            :   192.168.0.2
 Hello Interval        :       30 sec
 Hello HoldTime        :        105 sec
 Triggered Hello Delay :          5 sec
 Join/Prune Holdtime   :        210 sec
 Lan Prune Delay       :       Disabled
 Propagation Delay     :        500  ms
 Override Interval     :      2500  ms
 Graft Retry Interval  :         3 sec
 Max Graft Retries     :          3
 State Refresh Ori Int :        60 sec

Console#
```

## ip pim hello-holdtime

This command configures the interval to wait for hello messages from a neighboring PIM router before declaring it dead. Use the **no** form to restore the default value.

### SYNTAX

**ip pim hello-holdtime** *seconds*

**no ip pim hello-interval**

*seconds* - The hold time for PIM hello messages. (Range: 1-65535)

### DEFAULT SETTING

105 seconds

### COMMAND MODE

Interface Configuration (VLAN)

#### COMMAND USAGE

The **ip pim hello-holdtime** should be greater than the value of ip pim hello-interval (page 1212).

#### EXAMPLE

```
Console(config-if)#ip pim hello-holdtime 210
Console(config-if)#
```

### ip pim hello-interval

This command configures the frequency at which PIM hello messages are transmitted. Use the **no** form to restore the default value.

#### SYNTAX

**ip pim hello-interval** *seconds*

**no pim hello-interval**

*seconds* - Interval between sending PIM hello messages. (Range: 1-65535)

#### DEFAULT SETTING

30 seconds

#### COMMAND MODE

Interface Configuration (VLAN)

#### COMMAND USAGE

Hello messages are sent to neighboring PIM routers from which this device has received probes, and are used to verify whether or not these neighbors are still active members of the multicast tree.

#### EXAMPLE

```
Console(config-if)#ip pim hello-interval 60
Console(config-if)#
```

### ip pim join-prune-holdtime

This command configures the hold time for the prune state. Use the **no** form to restore the default value.

#### SYNTAX

**ip pim join-prune-holdtime** *seconds*

**no ip pim join-prune-holdtime**

*seconds* - The hold time for the prune state. (Range: 0-65535)

#### DEFAULT SETTING

210 seconds

**COMMAND MODE**
Interface Configuration (VLAN)

**COMMAND USAGE**
The multicast interface that first receives a multicast stream from a particular source forwards this traffic to all other PIM interfaces on the router. If there are no requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The prune state is maintained until the join-prune-holdtime timer expires or a graft message is received for the forwarding entry.

**EXAMPLE**

```
Console(config-if)#ip pim join-prune-holdtime 60
Console(config-if)#
```

## ip pim lan-prune-delay

This command causes this device to inform downstream routers of how long it will wait before pruning a flow after receiving a prune request. Use the **no** form to disable this feature.

**SYNTAX**

[**no**] **ip pim lan-prune-delay**

**DEFAULT SETTING**
Disabled

**COMMAND MODE**
Interface Configuration (VLAN)

**COMMAND USAGE**

- When other downstream routers on the same VLAN are notified that this upstream router has received a prune request, they must send a Join to override the prune before the prune delay expires if they want to continue receiving the flow. The message generated by this command effectively prompts any downstream neighbors with hosts receiving the flow to reply with a Join message. If no join messages are received after the prune delay expires, this router will prune the flow.

- Prune delay is the sum of the effective propagation-delay and effective override-interval, where effective propagation-delay is the largest propagation-delay from those advertised by each neighbor (including this switch), and effective override-interval is the largest override-interval from those advertised by each neighbor (including this switch).

**EXAMPLE**

```
Console(config-if)#ip pim lan-prune-delay
Console(config-if)#
```

#### RELATED COMMANDS

ip pim override-interval (1214)
ip pim propagation-delay (1214)

### ip pim override-interval

This command configures the override interval, or the time it takes a downstream router to respond to a lan-prune-delay message. Use the **no** form to restore the default setting.

#### SYNTAX

**ip pim override-interval** *milliseconds*

**no ip pim override-interval**

*milliseconds* - The time required for a downstream router to respond to a lan-prune-delay message by sending back a Join message if it wants to continue receiving the flow referenced in the message. (Range: 500-6000 milliseconds)

#### DEFAULT SETTING

2500 milliseconds

#### COMMAND MODE

Interface Configuration (VLAN)

#### COMMAND USAGE

The override interval configured by this command and the propagation delay configured by the ip pim propagation-delay command are used to calculate the LAN prune delay. If a downstream router has group members which want to continue receiving the flow referenced in a LAN prune delay message, then the override interval represents the time required for the downstream router to process the message and then respond by sending a Join message back to the upstream router to ensure that the flow is not terminated.

#### EXAMPLE

```
Console(config-if)#ip pim override-interval 3500
Console(config-if)#
```

#### RELATED COMMANDS

ip pim propagation-delay (1214)
ip pim lan-prune-delay (1213)

### ip pim propagation-delay

This command configures the propagation delay required for a LAN prune delay message to reach downstream routers. Use the **no** form to restore the default setting.

**ip pim propagation-delay** *milliseconds*

**no ip pim propagation-delay**

*milliseconds* - The time required for a lan-prune-delay message to reach downstream routers attached to the same VLAN interface. (Range: 100-5000 milliseconds)

**DEFAULT SETTING**
500 milliseconds

**COMMAND MODE**
Interface Configuration (VLAN)

**COMMAND USAGE**
The override interval configured by the ip pim override-interval command and the propagation delay configured by this command are used to calculate the LAN prune delay. If a downstream router has group members which want to continue receiving the flow referenced in a LAN prune delay message, then the propagation delay represents the time required for the lan-prune-delay message to be propagated down from the upstream router to all downstream routers attached to the same VLAN interface.

**EXAMPLE**

```
Console(config-if)#ip pim propagation-delay 600
Console(config-if)#
```

**RELATED COMMANDS**
ip pim override-interval (1214)
ip pim lan-prune-delay (1213)

## ip pim trigger-hello-delay

This command configures the maximum time before transmitting a triggered PIM Hello message after the router is rebooted or PIM is enabled on an interface. Use the **no** form to restore the default value.

**SYNTAX**

**ip pim trigger-hello-delay** *seconds*

**no ip pim trigger-hello-delay**

*seconds* - The maximum time before sending a triggered PIM Hello message. (Range: 0-5 seconds)

**DEFAULT SETTING**
5 seconds

**COMMAND MODE**
Interface Configuration (VLAN)

**COMMAND USAGE**
- When a router first starts or PIM is enabled on an interface, the hello delay is set to random value between 0 and the trigger-hello-delay. This prevents synchronization of Hello messages on multi-access links if multiple routers are powered on simultaneously.

■Also, if a Hello message is received from a new neighbor, the receiving router will send its own Hello message after a random delay between 0 and the trigger-hello-delay.

**EXAMPLE**

```
Console(config-if)#ip pim trigger-hello-delay 3
Console(config-if)#
```

## show ip pim interface

This command displays information about interfaces configured for PIM.

**SYNTAX**

**show ip pim interface** [**vlan** *vlan-id*]

*vlan-id* - VLAN ID (Range: 1-4094)

**COMMAND MODE**

Normal Exec, Privileged Exec

**COMMAND USAGE**

This command displays the PIM settings for the specified interface as described in the preceding pages. It also shows the address of the designated PIM router and the number of neighboring PIM routers.

**EXAMPLE**

```
Console#show ip pim interface vlan 1
PIM is enabled.
Vlan 1 is up.
 PIM Mode              :    Dense Mode
 IP Address            :    192.168.0.2
 Hello Interval        :    30 sec
 Hello HoldTime        :    105 sec
 Triggered Hello Delay :    5 sec
 Join/Prune Holdtime   :    210 sec
 Lan Prune Delay       :    Disabled
 Propagation Delay     :    500  ms
 Override Interval     :    2500  ms
 Graft Retry Interval  :    3 sec
 Max Graft Retries     :    3
 State Refresh Ori Int :    60 sec

Console#
```

## show ip pim neighbor

This command displays information about PIM neighbors.

**SYNTAX**

**show ip pim neighbor** [**interface vlan** *vlan-id*]

*vlan-id* - VLAN ID (Range: 1-4094)

### DEFAULT SETTING
Displays information for all known PIM neighbors.

### COMMAND MODE
Normal Exec, Privileged Exec

### EXAMPLE

```
Console#show ip pim neighbor
Neighbor Address VLAN Interface Uptime (sec.) Expiration Time (sec)
---------------- -------------- ------------- ---------------------
192.168.0.3/32   1          00:00:21     00:01:30
Console#
```

**Table 8: show ip pim neighbor** - display description

| Field | Description |
|---|---|
| Neighbor Address | IP address of the next-hop router. |
| VLAN Interface | Interface number that is attached to this neighbor. |
| Uptime | The duration this entry has been active. |
| Expiration Time | The time before this entry will be removed. |

## ip pim graft-retry-interval

This command configures the time to wait for a Graft acknowledgement before resending a Graft. Use the **no** form to restore the default value.

### SYNTAX

**ip pim graft-retry-interval** *seconds*

**no ip pim graft-retry-interval**

*seconds* - The time before resending a Graft. (Range: 1-10 seconds)

### DEFAULT SETTING
3 seconds

### COMMAND MODE
Interface Configuration (VLAN)

### COMMAND USAGE
A graft message is sent by a router to cancel a prune state. When a router receives a graft message, it must respond with an graft acknowledgement message. If this acknowledgement message is lost, the router that sent the graft message will resend it a number of times (as defined by the ip pim max-graft-retries command).

### EXAMPLE

```
Console(config-if)#ip pim graft-retry-interval 9
Console(config-if)#
```

## ip pim max-graft-retries

This command configures the maximum number of times to resend a Graft message if it has not been acknowledged. Use the **no** form to restore the default value.

### SYNTAX

**ip pim max-graft-retries** *retries*

**no ip pim max-graft-retries**

*retries* - The maximum number of times to resend a Graft. (Range: 1-10)

### DEFAULT SETTING

3

### COMMAND MODE

Interface Configuration (VLAN)

### EXAMPLE

```
Console(config-if)#ip pim max-graft-retries 5
Console(config-if)#
```

## ip pim state-refresh origination-interval

This command sets the interval between sending PIM-DM state refresh control messages. Use the **no** form to restore the default value.

### SYNTAX

**ip pim state-refresh origination-interval** *seconds*

**no ip pim max-graft-retries**

*seconds* - The interval between sending PIM-DM state refresh control messages. (Range: 1-100 seconds)

### DEFAULT SETTING

60 seconds

### COMMAND MODE

Interface Configuration (VLAN)

### COMMAND USAGE

- The pruned state times out approximately every three minutes and the entire PIM-DM network is reflooded with multicast packets and prune messages. The state refresh feature keeps the pruned state from timing out by periodically forwarding a control message down the distribution tree, refreshing the prune state on the outgoing interfaces of each router in the tree. This also enables PIM routers to recognize topology changes (sources joining or leaving a multicast group) before the default three-minute state timeout expires.

- This command is only effectively for interfaces of first hop, PIM-DM routers that are directly connected to the sources of multicast groups.

### EXAMPLE

```
Console(config-if)#ip pim state-refresh origination-interval 30
Console(config-if)#
```

## ip pim bsr-candidate

This command configures the switch as a Bootstrap Router (BSR) candidate. Use the **no** form to restore the default value.

### SYNTAX

**ip pim bsr-candidate interface vlan** *vlan-id* [**hash** *hash-mask-length*] [**priority** *priority*]

**no ip pim bsr-candidate**

*vlan-id* - VLAN ID (Range: 1-4094)

*hash-mask-length* - Hash mask length (in bits) used for RP selection (see ip pim rp-candidate and ip pim rp-address). The portion of the hash specified by the mask length is ANDed with the group address. Therefore, when the hash function is executed on any BSR, all groups with the same seed hash will be mapped to the same RP. If the mask length is less than 32, then only the first portion of the hash is used, and a single RP will be defined for multiple groups. (Range: 0-32 bits)

*priority* - Priority used by the candidate bootstrap router in the election process. The BSR candidate with the largest priority is preferred. If the priority values are the same, the candidate with the larger IP address is elected to be the BSR. Setting the priority to zero means that this router is not eligible to server as the BSR. At least one router in the PIM-SM domain must be set to a value greater than zero. (Range: 0-255)

### DEFAULT SETTING

Hash Mask Length: 10
Priority: 0

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- When the **ip pim bsr-candidate** command is entered, the router starts sending bootstrap messages to all of its PIM-SM neighbors. The IP address of the designated VLAN is sent as the candidate's BSR address. Each neighbor receiving the bootstrap message compares the BSR address with the address from previous messages. If the current address is the same or a higher address, it accepts the bootstrap message and forwards it. Otherwise, it drops the message.

- This router will continue to be the BSR until it receives a bootstrap message from another candidate with a higher priority (or a higher IP address if the priorities are the same).

- To improve failover recovery, it is advisable to select at least two core routers in diverse locations, each to serve as both a candidate BSR and candidate RP. It is also preferable to set up one of these routers as both the primary BSR and RP.

### EXAMPLE

The following example configures the router to start sending bootstrap messages out of the interface for VLAN 1 to all of its PIM-SM neighbors.

```
Console(config)#ip pim bsr-candidate interface vlan 1 hash 20 priority 200
Console(config)#exit
Console#show ip pim bsr-router
PIMv2 Bootstrap information
BSR address     : 192.168.0.2/32
Uptime          : 00:00:08
BSR Priority    : 200
Hash mask length : 20
Expire          : 00:00:57
Role            : Candidate BSR
State           : Elected BSR
Console#
```

## ip pim register-rate-limit

This command configures the rate at which register messages are sent by the Designated Router (DR) for each (source, group) entry. Use the **no** form to restore the default value.

### SYNTAX

**ip pim register-rate-limit** *rate*

**no ip pim register-rate-limit**

*rate* - The maximum number of register packets per second. (Range: 1-65535: Default: 0, which means no limit)

### DEFAULT SETTING

0

### COMMAND MODE

Global Configuration

### COMMAND USAGE

This command can be used to relieve the load on the Designated Router (DR) and RP. However, because register messages exceeding the limit are dropped, some receivers may experience data packet loss within the first few seconds in which register messages are sent from bursty sources.

### EXAMPLE

This example sets the register rate limit to 500 pps.

```
Console(config)#ip pim register-rate-limit 500
Console(config)#
```

## ip pim register-source

This command configures the IP source address of a register message to an address other than the outgoing interface address of the designated router (DR) that leads back toward the rendezvous point (RP). Use the **no** form to restore the default setting.

### SYNTAX

**ip pim register-source interface vlan** *vlan-id*

**no ip pim register-source**

*vlan-id* - VLAN ID (Range: 1-4094)

### DEFAULT SETTING

The IP address of the DR's outgoing interface that leads back to the RP

### COMMAND MODE

Global Configuration

### COMMAND USAGE

When the source address of a register message is filtered by intermediate network devices, or is not a uniquely routed address to which the RP can send packets, the replies sent from the RP to the source address will fail to reach the DR, resulting in PIM-SM protocol failures. This command can be used to overcome this type of problem by manually configuring the source address of register messages to an interface that leads back to the RP.

### EXAMPLE

This example sets the register rate limit to 500 pps.

```
Console(config)#ip pim register-source interface vlan 1
Console(config)#
```

## ip pim rp-address

This command sets a static address for the Rendezvous Point (RP) for a particular multicast group. Use the **no** form to remove an RP address or an RP address for a specific group.

### SYNTAX

[**no**] **ip pim rp-address** *rp-address* [**group-prefix** *group-address mask*]

*rp-address* - Static IP address of the router that will be an RP for the specified multicast group(s).

*group-address* - An IP multicast group address. If a group address is not specified, the RP is used for all multicast groups.

*mask* - Subnet mask that is used for the group address.

### DEFAULT SETTING

None

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- The router specified by this command will act as an RP for all multicast groups in the local PIM-SM domain if no groups are specified. A static RP can either be configured for the whole multicast group range 224.0.0.0/4, or for specific group ranges.

- Using this command to configure multiple static RPs with the same RP address is not allowed. If an IP address is specified that was previously used for an RP, then the older entry is replaced.

- Multiple RPs can be defined for different groups or group ranges. If a group is matched by more than one entry, the router will use the RP associated with the longer group prefix length. If the prefix lengths are the same, then the static RP with the highest IP address is chosen.

- Static definitions for RP addresses may be used together with RP addresses dynamically learned through the bootstrap router (BSR). If an RP address learned by the BSR and one statically configured using this command are both available for a group range, the RP address learned by the BSR is chosen over the one statically configured with this command.

- All routers within the same PIM-SM domain must be configured with the same RP(s). Selecting an RP through the dynamic election process is therefore preferable for most situations. Using the dynamic RP election process also allows a backup RP to automatically take over if the active RP router becomes unavailable.

- If the **no** form of this command is used without specifying a multicast group, the default 224.0.0.0 (with the mask 240.0.0.0) is removed. In other words, all multicast groups are removed.

### EXAMPLE

In the following example, the first PIM-SM command just specifies the RP address 192.168.1.1 to indicate that it will be used to service all multicast groups. The second PIM-SM command includes the multicast groups to be serviced by the RP.

```
Console(config)#ip pim rp-address 192.168.1.1
Console(config)#ip pim rp-address 192.168.2.1 group-prefix 224.9.0.0 255.255.0.0
Console(config)#end
Console#show ip pim rp mapping
PIM Group-to-RP Mappings
Groups          : 224.0.0.0/4
RP address      : 192.168.1.1/32
Info source     : static
Uptime          : 00:00:33
Expire          : Never
Groups          : 224.9.0.0/16
RP address      : 192.168.2.1/32
Info source     : static
Uptime          : 00:00:21
Expire          : Never
Console#
```

## ip pim rp-candidate

This command configures the router to advertise itself as a Rendezvous Point (RP) candidate to the bootstrap router (BSR). Use the **no** form to remove this router as an RP candidate.

### SYNTAX

**ip pim rp-candidate interface vlan** *vlan-id* [**group-prefix** *group-address mask*] [**interval** *seconds*] [**priority** *value*]

**no ip pim rp-candidate interface vlan** *vlan-id*

*vlan-id* - VLAN ID (Range: 1-4094)

*group-address* - An IP multicast group address. If a group address is not specified, the RP is advertised for all multicast groups.

*mask* - Subnet mask that is used for the group address.

*seconds* - The interval at which this device advertises itself as an RP candidate. (Range: 60-16383 seconds)

*value* - Priority used by the candidate RP in the election process. The RP candidate with the largest priority is preferred. If the priority values are the same, the candidate with the larger IP address is elected to be the RP. Setting the priority to zero means that this router is not eligible to server as the RP. (Range: 0-255)

### DEFAULT SETTING

Interval: 60 seconds
Priority: 0

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- When the **ip pim rp-candidate** command is entered, the router periodically sends PIMv2 messages to the BSR advertising itself as a candidate RP for the specified group addresses. The IP address of the designated VLAN is sent as the candidate's RP address. The BSR places information about all of the candidate RPs in subsequent bootstrap messages. The BSR uses the RP-election hash algorithm to select an active RP for each group range. The election process is performed by the BSR only for its own use. Each PIM-SM router that receives the list of RP candidates from the BSR also elects an active RP for each group range using the same election process.

- The election process for each group is based on the following criteria:

  - Find all RPs with the most specific group range.

  - Select those with the highest priority (lowest priority value).

  - Compute a hash value based on the group address, RP address, priority, and hash mask included in the bootstrap messages.

  - If there is a tie, use the candidate RP with the highest IP address.

- This distributed election process provides faster convergence and minimal disruption when an RP fails. It also serves to provide load balancing by distributing groups across multiple RPs. Moreover, when an RP fails, the responsible RPs are re-elected on each router, and the groups automatically distributed to the remaining RPs.

- To improve failover recovery, it is advisable to select at least two core routers in diverse locations, each to serve as both a candidate BSR and candidate RP. It is also preferable to set up one of these routers as both the primary BSR and RP.

#### EXAMPLE

The following example configures the router to start advertising itself to the BSR as a candidate RP for the indicated multicast groups.

```
Console(config)#ip pim rp-candidate interface vlan 1 group-prefix 224.0.0.0 255.0.0.0
Console(config)#end
Console#show ip pim rp mapping
PIM Group-to-RP Mappings
Groups       : 224.0.0.0/8
RP address   : 192.168.0.2/32
Info source  : 192.168.0.2/32, via bootstrap, priority: 0
Uptime       : 00:00:51
Expire       : 00:01:39
Console#
```

## ip pim spt-threshold

This command prevents the last-hop PIM router from switching to Shortest Path Source Tree (SPT) mode. Use the **no** form to allow the router to switch over to SPT mode.

#### SYNTAX

**ip pim spt-threshold infinity** [**group-prefix** *group-address mask*]

**no ip pim spt-threshold infinity**

*group-address* - An IP multicast group address. If a group address is not specified, the command applies to all multicast groups.

*mask* - Subnet mask that is used for the group address.

#### DEFAULT SETTING

The last-hop PIM router joins the shortest path tree immediately after the first packet arrives from a new source

#### COMMAND MODE

Global Configuration

#### COMMAND USAGE

- The default path for packets from a multicast source to a receiver is through the RP. However, the path through the RP is not always the shortest path. Therefore, the router uses the RP to forward only the first packet from a new multicast group to its receivers. Afterwards, it calculates the shortest path tree (SPT) directly between the receiver and source, and then uses the SPT to send all subsequent packets from the source to the receiver instead of using the shared tree. Note that when the SPT threshold is not set by this command, the PIM leaf router will join the shortest path tree immediately after receiving the first packet from a new source.

- This command forces the router to use the shared tree for all multicast groups, or just for the specified multicast groups.

- Only one entry is allowed for this command.

### EXAMPLE

This example prevents the switch from using the SPT for multicast groups 224.1.0.0~224.1.255.255.

```
Console(config)#ip pim spt-threshold infinity group-prefix 224.1.0.0 0.0.255.255
Console#
```

## ip pim dr-priority

This command sets the priority value for a Designated Router (DR) candidate. Use the **no** form to restore the default setting.

### SYNTAX

**ip pim dr-priority** *priority-value*

**no ip pim dr-priority**

*priority-value* - Priority advertised by a router when bidding to become the DR. (Range: 0-4294967294)

### DEFAULT SETTING

1

### COMMAND MODE

Interface Configuration (VLAN)

### COMMAND USAGE

- More than one PIM-SM router may be connected to an Ethernet or other shared-media LAN. If multicast hosts are directly connected to the LAN, then only one of these routers is elected as the DR, and acts on behalf of these hosts, sending periodic Join/Prune messages toward a group-specific RP for each group. A single DR is elected per interface (LAN or otherwise) using a simple election process.

- The router with the highest priority configured on an interface is elected as the DR. If more than one router attached to this interface uses the same priority, then the router with the highest IP address is elected to serve as the DR.

- If a router does not advertise a priority in its hello messages, it is assumed to have the highest priority and is elected as the DR. If more than one router is not advertising its priority, then the router with the highest IP address is elected to serve as the DR.

### EXAMPLE

This example sets the priority used in the bidding process for the DR.

```
Console(config)#interface vlan 1
Console(config-if)#ip pim dr-priority 20
Console(config-if)#end
Console#show ip pim interface
PIM is enabled.
Vlan 1 is up.
 PIM Mode              :    Sparse Mode
 IP Address            :    192.168.0.2
 Hello Interval        :        30 sec
 Hello HoldTime        :        105 sec
 Triggered Hello Delay :          5 sec
 Join/Prune Holdtime   :        210 sec
 Lan Prune Delay       :       Disabled
 Propagation Delay     :        500  ms
 Override Interval     :       2500  ms
 DR Priority           :        20
 Join/Prune Interval   :        60 sec

Console#
```

## ip pim join-prune-interval

This command sets the join/prune timer. Use the **no** form to restore the default setting.

### SYNTAX

**ip pim join-prune-interval** *seconds*

**no ip pim join-prune-interval**

*seconds* - The interval at which join/prune messages are sent. (Range: 1-65535 seconds)

### DEFAULT SETTING

60 seconds

### COMMAND MODE

Interface Configuration (VLAN)

### COMMAND USAGE

- By default, the switch sends join/prune messages every 210 seconds to inform other PIM-SM routers about clients who want to join or leave a multicast group.

- Use the same join/prune message interval on all the PIM-SM routers in the same PIM-SM domain, otherwise the routing protocol's performance will be adversely affected.

- The multicast interface that first receives a multicast stream from a particular source forwards this traffic only to those interfaces on the router that have requested to join this group. When there are no longer any requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The protocol maintains both the current join state and the pending Reverse Path Tree (RPT) prune state for this (source, group) pair until the join/prune-interval timer expires.

### EXAMPLE

This example sets the priority used in the bidding process for the DR.

```
Console(config)#interface vlan 1
Console(config-if)#ip pim join-prune-interval 210
Console#show ip pim interface
PIM is enabled.
Vlan 1 is up.
 PIM Mode              :    Sparse Mode
 IP Address            :   192.168.0.2
 Hello Interval        :       30 sec
 Hello HoldTime        :        105 sec
 Triggered Hello Delay :            5 sec
 Join/Prune Holdtime   :         210 sec
 Lan Prune Delay       :       Disabled
 Propagation Delay     :          500  ms
 Override Interval     :       2500  ms
 DR Priority           :       20
 Join/Prune Interval   :          80 sec

Console#
```

## clear ip pim bsr rp-set

This command clears multicast group to RP mapping entries learned through the PIMv2 bootstrap router (BSR).

### COMMAND MODE

Privileged Exec

### COMMAND USAGE

- This command can be used to update entries in the static multicast forwarding table immediately after making configuration changes to the RP.
- Use the show ip pim rp mapping command to display active RPs that are cached with associated multicast routing entries.

### EXAMPLE

This example clears the RP map.

```
Console#clear ip pim bsr rp-set
Console#show ip pim rp mapping
PIM Group-to-RP Mappings
Console#
```

## show ip pim bsr-router

This command displays information about the bootstrap router (BSR).

### COMMAND MODE

Privileged Exec

### COMMAND USAGE

This command displays information about the elected BSR.

### EXAMPLE

This example displays information about the BSR.

```
Console#show ip pim bsr-router
PIMv2 Bootstrap information
BSR address      : 192.168.0.2/32
Uptime           : 01:01:23
BSR Priority     : 200
Hash mask length : 20
Expire           : 00:00:42
Role             : Candidate BSR
State            : Elected BSR
Console#
```

**Table 9: show ip pim bsr-router** - display description

| Field | Description |
|---|---|
| BSR address | IP address of interface configured as the BSR. |
| Uptime | The time this BSR has been up and running. |
| BSR Priority | Priority assigned to this interface for use in the BSR election process. |
| Hash mask length | The number of significant bits used in the multicast group comparison mask. This mask determines the multicast group for which this router can be a BSR. |
| Expire | The time before this entry will be removed. |
| Role | Candidate BSR or Non-candidate BSR. |
| State | Operation state of BSR includes:<br>◆ No information – No information stored for this device.<br>◆ Accept Any – The router does not know of an active BSR, and will accept the first bootstrap message it sees as giving the new BSR's identity and the RP-set.<br>◆ Accept Preferred – The router knows the identity of the current BSR, and is using the RP-set provided by that BSR. Only bootstrap messages from that BSR or from a C-BSR with higher weight than the current BSR will be accepted.<br>◆ Candidate BSR – Bidding in election process.<br>◆ Pending-BSR – The router is a candidate to be the BSR for the RP-set. Currently, no other router is the preferred BSR, but this router is not yet the elected BSR.<br>◆ Elected BSR – elected to serve as BSR |

## show ip pim rp mapping

This command displays active RPs and associated multicast routing entries.

### COMMAND MODE

Privileged Exec

### EXAMPLE

This example displays the RP map.

```
Console#show ip pim rp mapping
PIM Group-to-RP Mappings
Groups           : 224.0.0.0/8
```

```
RP address      : 192.168.0.2/32
Info source     : 192.168.0.2/32, via bootstrap, priority: 0
Uptime          : 00:31:09
Expire          : 00:02:21
Console#
```

**Table 10: show ip pim rp mapping** - display description

| Field | Description |
|---|---|
| Groups | The multicast group address, mask length managed by the RP. |
| RP address | IP address of the RP used for the listed multicast group |
| Info source | RP that advertised the mapping, how the RP was selected (Static or Bootstrap), and the priority used in the bidding process |
| Uptime | The time this RP has been up and running |
| Expire | The time before this entry will be removed |

## show ip pim rp-hash

This command displays the RP used for the specified multicast group, and the RP that advertised the mapping.

### SYNTAX

**show ip pim rp-hash** *group-address*

*group-address* - An IP multicast group address.

### COMMAND MODE

Privileged Exec

### EXAMPLE

This example displays the RP used for the specified group.

```
Console#show ip pim rp-hash 224.0.1.3
RP address        : 224.0.1.3
Info source       : 192.168.0.2/32, via (null)
Console#
```

**Table 11: show ip pim rp-hash** - display description

| Field | Description |
|---|---|
| RP address | IP address of the RP used for the specified multicast group |
| Info source | RP that advertised the mapping, and how the RP was selected |

## IPv6 PIM COMMANDS

This section describes commands used to configure IPv6 PIM-DM dynamic multicast routing on the switch.

**Table 12: PIM-DM and PIM-SM Multicast Routing Commands**

| Command | Function | Mode |
|---|---|---|
| router pim6 | Enables IPv6 PIM globally for the router | GC |
| ipv6 pim dense-mode | Enables PIM-DM on the specified interface | IC |
| ipv6 pim graft-retry-interval | Configures the time to wait for a Graft acknowledgement before resending a Graft message | IC |
| ipv6 pim hello-holdtime | Sets the time to wait for hello messages from a neighboring PIM router before declaring it dead | IC |
| ipv6 pim hello-interval | Sets the interval between sending PIM hello messages | IC |
| ipv6 pim join-prune-holdtime | Configures the hold time for the prune state | IC |
| ipv6 pim lan-prune-delay | Informs downstream routers of the delay before it prunes a flow after receiving a prune request | IC |
| ipv6 pim max-graft-retries | Configures the maximum number of times to resend a Graft message if it has not been acknowledged | IC |
| ipv6 pim override-interval | Specifies the time it takes a downstream router to respond to a lan-prune-delay message | IC |
| ipv6 pim propagation-delay | Configures the propagation delay required for a LAN prune delay message to reach downstream routers | IC |
| ipv6 pim state-refresh origination-interval | Sets the interval between PIM-DM state refresh control messages | IC |
| ipv6 pim trigger-hello-delay | Configures the trigger hello delay | IC |
| show ipv6 pim interface | Displays information about interfaces configured for PIM | NE, PE |
| show ip pim neighbor | Displays information about PIM neighbors | NE, PE |

## router pim6

This command enables IPv6 Protocol-Independent Multicast routing globally on the router. Use the **no** form to disable PIM multicast routing.

### SYNTAX

[**no**] **router pim6**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Global Configuration

### COMMAND USAGE

- This command enables IPv6 PIM-DM globally for the router. You also need to enable IPv6 PIM-DM for each interface that will support multicast routing using the ipv6 pim dense-mode command, and make any changes necessary to the multicast protocol parameters.
- To use multicast routing, IGMP proxy can not enabled on any interface of the device (see the ip igmp proxy command).

### EXAMPLE

```
Console(config)#router pim6
Console(config)#
```

## ipv6 pim dense-mode

This command enables IPv6 PIM-DM on the specified interface. Use the **no** form to disable IPv6 PIM-DM on this interface.

### SYNTAX

[**no**] **ipv6 pim dense-mode**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Interface Configuration (VLAN)

### COMMAND USAGE

- To fully enable PIM, you need to enable multicast routing globally for the router with the ip multicast-routing command, enable PIM globally for the router with the router pim6 command, and also enable PIM-DM for each interface that will participate in multicast routing with this command.

- If you enable PIM on an interface, you should also enable IGMP on that interface. PIM mode selection determines how the switch populates the multicast routing table, and how it forwards packets received from directly connected LAN interfaces.Dense mode interfaces are always added to the multicast routing table.

- Dense-mode interfaces are subject to multicast flooding by default, and are only removed from the multicast routing table when the router determines that there are no group members or downstream routers, or when a prune message is received from a downstream router.

### EXAMPLE

```
Console(config)#interface vlan 1

Console(config-if)#end
Console#show ipv6 pim interface
PIM is enabled.
Vlan 1 is up.
 PIM Mode                 : Dense Mode
 IPv6 Address             : None
 Hello Interval           : 30 sec
 Hello HoldTime           : 105 sec
 Triggered Hello Delay    : 5 sec
 Join/Prune Holdtime      : 210 sec
 Lan Prune Delay          : Disabled
 Propagation Delay        : 500  ms
 Override Interval        : 2500  ms
 Graft Retry Interval     : 3 sec
 Max Graft Retries        : 3
 State Refresh Ori Int    : 60 sec
```

```
Console#
```

## ipv6 pim graft-retry-interval

This command configures the time to wait for a Graft acknowledgement before resending a Graft. Use the **no** form to restore the default value.

### Syntax

**ipv6 pim graft-retry-interval** *seconds*

**no ipv6 pim graft-retry-interval**

*seconds* - The time before resending a Graft. (Range: 1-10 seconds)

### Default Setting

3 seconds

### Command Mode

Interface Configuration (VLAN)

### Command Usage

A graft message is sent by a router to cancel a prune state. When a router receives a graft message, it must respond with an graft acknowledgement message. If this acknowledgement message is lost, the router that sent the graft message will resend it a number of times (as defined by the ipv6 pim max-graft-retries command).

### Example

```
Console(config-if)#ipv6 pim graft-retry-interval 9
Console(config-if)#
```

## ipv6 pim hello-holdtime

This command configures the interval to wait for hello messages from a neighboring PIM router before declaring it dead. Use the **no** form to restore the default value.

### Syntax

**ipv6 pim hello-holdtime** *seconds*

**no ipv6 pim hello-interval**

*seconds* - The hold time for PIM hello messages. (Range: 1-65535)

### Default Setting

105 seconds

### Command Mode

Interface Configuration (VLAN)

### Command Usage

The **ip pim hello-holdtime** should be greater than the value of ipv6 pim hello-interval.

#### EXAMPLE

```
Console(config-if)#ipv6 pim hello-holdtime 210
Console(config-if)#
```

### ipv6 pim hello-interval

This command configures the frequency at which PIM hello messages are transmitted. Use the **no** form to restore the default value.

#### SYNTAX

**ipv6 pim hello-interval** *seconds*

**no pimv6 hello-interval**

*seconds* - Interval between sending PIM hello messages. (Range: 1-65535)

#### DEFAULT SETTING

30 seconds

#### COMMAND MODE

Interface Configuration (VLAN)

#### COMMAND USAGE

Hello messages are sent to neighboring PIM routers from which this device has received probes, and are used to verify whether or not these neighbors are still active members of the multicast tree.

#### EXAMPLE

```
Console(config-if)#ipv6 pim hello-interval 60
Console(config-if)#
```

### ipv6 pim join-prune-holdtime

This command configures the hold time for the prune state. Use the **no** form to restore the default value.

#### SYNTAX

**ipv6 pim join-prune-holdtime** *seconds*

**no ipv6 pim join-prune-holdtime**

*seconds* - The hold time for the prune state. (Range: 0-65535)

#### DEFAULT SETTING

210 seconds

#### COMMAND MODE

Interface Configuration (VLAN)

### COMMAND USAGE

The multicast interface that first receives a multicast stream from a particular source forwards this traffic to all other PIM interfaces on the router. If there are no requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The prune state is maintained until the join-prune-holdtime timer expires or a graft message is received for the forwarding entry.

### EXAMPLE

```
Console(config-if)#ipv6 pim join-prune-holdtime 60
Console(config-if)#
```

## ipv6 pim lan-prune-delay

This command causes this device to inform downstream routers of how long it will wait before pruning a flow after receiving a prune request. Use the **no** form to disable this feature.

### SYNTAX

[**no**] **ipv6 pim lan-prune-delay**

### DEFAULT SETTING

Disabled

### COMMAND MODE

Interface Configuration (VLAN)

### COMMAND USAGE

- When other downstream routers on the same VLAN are notified that this upstream router has received a prune request, they must send a Join to override the prune before the prune delay expires if they want to continue receiving the flow. The message generated by this command effectively prompts any downstream neighbors with hosts receiving the flow to reply with a Join message. If no join messages are received after the prune delay expires, this router will prune the flow.

- Prune delay is the sum of the effective propagation-delay and effective override-interval, where effective propagation-delay is the largest propagation-delay from those advertised by each neighbor (including this switch), and effective override-interval is the largest override-interval from those advertised by each neighbor (including this switch).

### EXAMPLE

```
Console(config-if)#ipv6 pim lan-prune-delay
Console(config-if)#
```

### RELATED COMMANDS

ipv6 pim override-interval (1235)
ipv6 pim propagation-delay (1236)

## ipv6 pim max-graft-retries

This command configures the maximum number of times to resend a Graft message if it has not been acknowledged. Use the **no** form to restore the default value.

### SYNTAX

**ipv6 pim max-graft-retries** *retries*

**no ipv6 pim max-graft-retries**

*retries* - The maximum number of times to resend a Graft. (Range: 1-10)

### DEFAULT SETTING

3

### COMMAND MODE

Interface Configuration (VLAN)

### EXAMPLE

```
Console(config-if)#ipv6 pim max-graft-retries 5
Console(config-if)#
```

## ipv6 pim override-interval

This command configures the override interval, or the time it takes a downstream router to respond to a lan-prune-delay message. Use the **no** form to restore the default setting.

### SYNTAX

**ipv6 pim override-interval** *milliseconds*

**no ipv6 pim override-interval**

*milliseconds* - The time required for a downstream router to respond to a lan-prune-delay message by sending back a Join message if it wants to continue receiving the flow referenced in the message. (Range: 500-6000 milliseconds)

### DEFAULT SETTING

2500 milliseconds

### COMMAND MODE

Interface Configuration (VLAN)

### COMMAND USAGE

The override interval configured by this command and the propagation delay configured by the ipv6 pim propagation-delay command are used to calculate the LAN prune delay. If a downstream router has group members which want to continue receiving the flow referenced in a LAN prune delay message, then the override interval represents the time required for the downstream router to process the message and then respond by sending a Join message back to the upstream router to ensure that the flow is not terminated.

### EXAMPLE

```
Console(config-if)#ipv6 pim override-interval 3500
Console(config-if)#
```

### RELATED COMMANDS

ipv6 pim propagation-delay (1236)
ipv6 pim lan-prune-delay (1234)

## ipv6 pim propagation-delay

This command configures the propagation delay required for a LAN prune delay message to reach downstream routers. Use the **no** form to restore the default setting.

**ipv6 pim propagation-delay** *milliseconds*

**no ipv6 pim propagation-delay**

*milliseconds* - The time required for a lan-prune-delay message to reach downstream routers attached to the same VLAN interface. (Range: 100-5000 milliseconds)

### DEFAULT SETTING

500 milliseconds

### COMMAND MODE

Interface Configuration (VLAN)

### COMMAND USAGE

The override interval configured by the ipv6 pim override-interval command and the propagation delay configured by this command are used to calculate the LAN prune delay. If a downstream router has group members which want to continue receiving the flow referenced in a LAN prune delay message, then the propagation delay represents the time required for the lan-prune-delay message to be propagated down from the upstream router to all downstream routers attached to the same VLAN interface.

### EXAMPLE

```
Console(config-if)#ipv6 pim propagation-delay 600
Console(config-if)#
```

### RELATED COMMANDS

ipv6 pim override-interval (1235)
ipv6 pim lan-prune-delay (1234)

## ipv6 pim state-refresh origination-interval

This command sets the interval between sending PIM-DM state refresh control messages. Use the **no** form to restore the default value.

### SYNTAX

**ipv6 pim state-refresh origination-interval** *seconds*

**no ipv6 pim max-graft-retries**

*seconds* - The interval between sending PIM-DM state refresh control messages. (Range: 1-100 seconds)

### DEFAULT SETTING
60 seconds

### COMMAND MODE
Interface Configuration (VLAN)

### COMMAND USAGE
- The pruned state times out approximately every three minutes and the entire PIM-DM network is reflooded with multicast packets and prune messages. The state refresh feature keeps the pruned state from timing out by periodically forwarding a control message down the distribution tree, refreshing the prune state on the outgoing interfaces of each router in the tree. This also enables PIM routers to recognize topology changes (sources joining or leaving a multicast group) before the default three-minute state timeout expires.

- This command is only effectively for interfaces of first hop, PIM-DM routers that are directly connected to sources of multicast groups.

### EXAMPLE
```
Console(config-if)#ipv6 pim state-refresh origination-interval 30
Console(config-if)#
```

## ipv6 pim trigger-hello-delay

This command configures the maximum time before transmitting a triggered PIM Hello message after the router is rebooted or PIM is enabled on an interface. Use the **no** form to restore the default value.

### SYNTAX
**ipv6 pim trigger-hello-delay** *seconds*

**no ipv6 pim trigger-hello-delay**

*seconds* - The maximum time before sending a triggered PIM Hello message. (Range: 0-5)

### DEFAULT SETTING
5 seconds

### COMMAND MODE
Interface Configuration (VLAN)

### COMMAND USAGE
- When a router first starts or PIM is enabled on an interface, the hello delay is set to random value between 0 and the trigger-hello-delay. This prevents synchronization of Hello messages on multi-access links if multiple routers are powered on simultaneously.

- Also, if a Hello message is received from a new neighbor, the receiving router will send its own Hello message after a random delay between 0 and the trigger-hello-delay.

#### EXAMPLE

```
Console(config-if)#ipv6 pim trigger-hello-delay 3
Console(config-if)#
```

## show ipv6 pim interface

This command displays information about interfaces configured for PIM.

#### SYNTAX

**show ipv6 pim** [**interface vlan** *vlan-id*]

*vlan-id* - VLAN ID (Range: 1-4094)

#### COMMAND MODE

Normal Exec, Privileged Exec

#### COMMAND USAGE

This command displays the PIM settings for the specified interface as described in the preceding pages. It also shows the address of the designated PIM router and the number of neighboring PIM routers.

#### EXAMPLE

```
Console#show ip pim interface vlan 1
PIM is enabled.
Vlan 1 is up.
 PIM Mode                  : Dense Mode
 IPv6 Address              : None
 Hello Interval            : 30 sec
 Hello HoldTime            : 105 sec
 Triggered Hello Delay     : 5 sec
 Join/Prune Holdtime       : 210 sec
 Lan Prune Delay           : Disabled
 Propagation Delay         : 500  ms
 Override Interval         : 2500  ms
 Graft Retry Interval      : 3 sec
 Max Graft Retries         : 3
 State Refresh Ori Int     : 60 sec

Console#
```

## show ipv6 pim neighbor

This command displays information about PIM neighbors.

#### SYNTAX

**show ipv6 pim neighbor** [**interface vlan** *vlan-id*]

*vlan-id* - VLAN ID (Range: 1-4094)

### Default Setting
Displays information for all known PIM neighbors.

### Command Mode
Normal Exec, Privileged Exec

### Example

```
Console#show ipv6 pim neighbor
Address                                  VLAN Interface   Uptime   Expire
---------------------------------------- ---------------- -------- --------
 FF80::0101                                VLAN 1         00:01:23 00:01:23
 FF80::0202                                VLAN 2         1d 11h   Never

Console#
```

**Table 13: show ipv6 pim neighbor** - display description

| Field | Description |
|---|---|
| Neighbor Address | IP address of the next-hop router. |
| VLAN Interface | Interface number that is attached to this neighbor. |
| Uptime | The duration this entry has been active. |
| Expiration Time | The time before this entry will be removed. |

# APPENDICES

This section provides additional information and includes these items:

# AX SOFTWARE SPECIFICATIONS

## SOFTWARE FEATURES

| | |
|---|---|
| **MANAGEMENT AUTHENTICATION** | **Local, RADIUS, TACACS+, Port Authentication (802.1X), HTTPS, SSH, Port Security, IP Filter** |
| **GENERAL SECURITY MEASURES** | **Access Control Lists (256 ACLs – 96 MAC rules, 96 IP rules, 96 IPv6 rules), Port Authentication (802.1X), MAC Authentication, Port Security, DHCP Snooping, IP Source Guard** |
| **PORT CONFIGURATION** | **1000BASE-T: 10/100 Mbps at half/full duplex, 1000 Mbps at full duplex**<br>1000BASE-SX/LX/LH - 1000 Mbps at full duplex (SFP)<br>10GBASE-SR/LR/ER - 10 Gbps at full duplex (Module)<br>10GBASE-T - 10 Gbps,1000 Mbps, 100 Mbps at full duplex (Module) |
| **FLOW CONTROL** | Full Duplex: IEEE 802.3-2005<br>Half Duplex: Back pressure |
| **STORM CONTROL** | **Broadcast traffic throttled above a critical threshold** |
| **PORT MIRRORING** | **26 sessions, one or more source ports to one destination port** |
| **RATE LIMITS** | **Input/Output Limits**<br>**Range configured per port** |
| **PORT TRUNKING** | **Static trunks (Cisco EtherChannel compliant)**<br>**Dynamic trunks (Link Aggregation Control Protocol)** |
| **SPANNING TREE ALGORITHM** | **Spanning Tree Protocol (STP, IEEE 802.1D-2004)**<br>**Rapid Spanning Tree Protocol (RSTP, IEEE 802.1D-2004)**<br>**Multiple Spanning Tree Protocol (MSTP, IEEE 802.1D-2004)** |

| | |
|---|---|
| **VLAN SUPPORT** | **Up to 4093 groups; port-based, protocol-based, tagged (802.1Q), private VLANs, voice VLANs, IP subnet, MAC-based, QinQ tunnel, GVRP for automatic VLAN learning** |
| **CLASS OF SERVICE** | **Supports eight levels of priority**<br>**Strict, Weighted Round Robin, or hybrid queuing**<br>**Layer 3/4 priority mapping: IP Port, IP Precedence, IP DSCP** |
| **QUALITY OF SERVICE** | **DiffServ[1] supports class maps, policy maps, and service policies** |
| **MULTICAST FILTERING** | **IGMP Snooping (Layer 2)**<br>**IGMP (Layer 3)**<br>**IGMP Proxy**<br>**Multicast VLAN Registration** |
| **IP ROUTING** | **ARP, Proxy ARP**<br>**Static routes**<br>**CIDR (Classless Inter-Domain Routing)**<br>**RIP, RIPv2, OSPFv2, OSPFv3 unicast routing**<br>**PIM-SM, PIM-DM, PIMv6 multicast routing**<br>**VRRP (Virtual Router Redundancy Protocol)** |
| **ADDITIONAL FEATURES** | **BOOTP Client**<br>**DHCP Client, Relay, Option 82, Server**<br>**DNS Client, Proxy**<br>**LLDP (Link Layer Discover Protocol)**<br>**RMON (Remote Monitoring, groups 1,2,3,9)**<br>**SMTP Email Alerts**<br>**SNMP (Simple Network Management Protocol)**<br>**SNTP (Simple Network Time Protocol)** |

## MANAGEMENT FEATURES

| | |
|---|---|
| **IN-BAND MANAGEMENT** | **Telnet, web-based HTTP or HTTPS, SNMP manager, or Secure Shell** |
| **OUT-OF-BAND MANAGEMENT** | **RS-232 DB-9 console port** |

1. Currently only supported for IPv4. Will be supported for IPv6 in future release.

**SOFTWARE LOADING** HTTP, FTP or TFTP in-band, or XModem out-of-band

**SNMP** Management access via MIB database
Trap management to specified hosts

**RMON** Groups 1, 2, 3, 9 (Statistics, History, Alarm, Event)

## STANDARDS

IEEE 802.1AB Link Layer Discovery Protocol
IEEE 802.1D-2004 Spanning Tree Algorithm and traffic priorities
- Spanning Tree Protocol
- Rapid Spanning Tree Protocol
- Multiple Spanning Tree Protocol

IEEE 802.1p Priority tags
IEEE 802.1Q VLAN
IEEE 802.1v Protocol-based VLANs
IEEE 802.1X Port Authentication
IEEE 802.3-2005
- Ethernet, Fast Ethernet, Gigabit Ethernet, and
- 10 Gigabit Ethernet (fiber and short-haul copper)
- Link Aggregation Control Protocol (LACP)
- Full-duplex flow control (ISO/IEC 8802-3)

IEEE 802.3ac VLAN tagging
ARP (RFC 826)
DHCP Client (RFC 2131)
DHCP Relay (RFC 951, 2132, 3046)
DHCP Server (RFC 2131, 2132)
HTTPS
ICMP (RFC 792)
IGMP (RFC 1112)
IGMPv2 (RFC 2236)
IGMPv3 (RFC 3376) - partial support
IGMP Proxy (RFC 4541)
IPv4 IGMP (RFC 3228)
OSPF (RFC 2328, 2178, 1587)
OSPFv3 (RFC 2740)
RADIUS+ (RFC 2618)
RIPv1 (RFC 1058)
RIPv2 (RFC 2453)
RIPv2, extension (RFC 1724)
RMON (RFC 2819 groups 1,2,3,9)

**SNMP (RFC 1157)**
**SNMPv2c (RFC 1901, 2571)**
**SNMPv3 (RFC DRAFT 2273, 2576, 3410, 3411, 3413, 3414, 3415)**
**SNTP (RFC 2030)**
**SSH (Version 2.0)**
**TELNET (RFC 854, 855, 856)**
**TFTP (RFC 1350)**
**VRRP (RFC 5798)**

## MANAGEMENT INFORMATION BASES

**Bridge MIB (RFC 1493)**
**Differentiated Services MIB (RFC 3289)**
**DNS Resolver MIB (RFC 1612)**
**Entity MIB (RFC 2737)**
**Ether-like MIB (RFC 2665)**
**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 MIB (RFC 2011)**
**IP Forwarding Table MIB (RFC 2096)**
**IP Multicasting related MIBs**
**IPV6-MIB (RFC 2065)**
**IPV6-ICMP-MIB (RFC 2066)**
**IPV6-TCP-MIB (RFC 2052)**
**IPV6-UDP-MIB (RFC2054)**
**MAU MIB (RFC 3636)**
**MIB II (RFC 1213)**
**OSPF MIB (RFC 1850)**
**OSPFv3 MIB (draft-ietf-ospf-ospfv3-mib-15.txt)**
**P-Bridge MIB (RFC 2674P)**
**Port Access Entity MIB (IEEE 802.1X)**
**Port Access Entity Equipment MIB**
**Private MIB**
**Q-Bridge MIB (RFC 2674Q)**
**QinQ Tunneling (IEEE 802.1ad Provider Bridges)**
**Quality of Service MIB**
**RADIUS Accounting Server MIB (RFC 2621)**
**RADIUS Authentication Client MIB (RFC 2619)**
**RIP1 MIB (RFC 1058)**

**RIP2 MIB (RFC 2453)**
**RIP2 Extension (RFC1724)**
**RMON MIB (RFC 2819)**
**RMON II Probe Configuration Group (RFC 2021, partial implementation)**
**SNMP Community MIB (RFC 3584)**
**SNMP Framework MIB (RFC 3411)**
**SNMP-MPD MIB (RFC 3412)**
**SNMP Target MIB, SNMP Notification MIB (RFC 3413)**
**SNMP User-Based SM MIB (RFC 3414)**
**SNMP View Based ACM MIB (RFC 3415)**
**SNMPv2 IP MIB (RFC 2011)**
**TACACS+ Authentication Client MIB**
**TCP MIB (RFC 2012)**
**Trap (RFC 1215)**
**UDP MIB (RFC 2013)**
**VRRP MIB (RFC 6527)**

# AY TROUBLESHOOTING

## PROBLEMS ACCESSING THE MANAGEMENT INTERFACE

**Table 1: Troubleshooting Chart**

| Symptom | Action |
|---|---|
| Cannot connect using Telnet, web browser, or SNMP software | ■ Be sure the switch is powered up.<br>■ Check network cabling between the management station and the switch.<br>■ Check that you have a valid network connection to the switch and that the port you are using has not been disabled.<br>■ Be sure you have configured the VLAN interface through which the management station is connected with a valid IP address, subnet mask and default gateway.<br>■ Be sure the management station has an IP address in the same subnet as the switch's IP interface to which it is connected.<br>■ If you are trying to connect to the switch via the IP address for a tagged VLAN group, your management station, and the ports connecting intermediate switches in the network, must be configured with the appropriate tag.<br>■ If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time. |
| Cannot connect using Secure Shell | ■ If you cannot connect using SSH, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time.<br>■ Be sure the control parameters for the SSH server are properly configured on the switch, and that the SSH client software is properly configured on the management station.<br>■ Be sure you have generated both an RSA and DSA public key on the switch, exported this key to the SSH client, and enabled SSH service.<br>■ Be sure you have set up an account on the switch for each SSH user, including user name, authentication level, and password.<br>■ Be sure you have imported the client's public key to the switch (if public key authentication is used). |
| Cannot access the on-board configuration program via a serial port connection | ■ Be sure you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity, and the baud rate set to 115200 bps).<br>■ Check that the serial cable conforms to the pin-out connections provided in the Installation Guide. |
| Forgot or lost the password | ■ Contact your local distributor. |

## USING SYSTEM LOGS

If a fault does occur, refer to the Installation Guide to ensure that the problem you encountered is actually caused by the switch. If the problem appears to be caused by the switch, follow these steps:

1. Enable logging.
2. Set the error messages reported to include all categories.
3. Enable SNMP.
4. Enable SNMP traps.
5. Designate the SNMP host that is to receive the error messages.
6. Repeat the sequence of commands or other actions that lead up to the error.
7. Make a list of the commands or circumstances that led to the fault. Also make a list of any error messages displayed.
8. Set up your terminal emulation software so that it can capture all console output to a file. Then enter the “show tech-support” command to record all system settings in this file.
9. Contact your distributor’s service engineer, and send a detailed description of the problem, along with the file used to record your system settings.

For example:

```
Console(config)#logging on
Console(config)#logging history flash 7
Console(config)#snmp-server host 192.168.1.23
:
```

# AZ LICENSE INFORMATION

This product includes copyrighted third-party software subject to the terms of the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other related free software licenses. The GPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, refer to the section “The GNU General Public License” below, or refer to the applicable license as included in the source-code archive.

## THE GNU GENERAL PUBLIC LICENSE

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

**Preamble**

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

**GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION**

1. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The “Program”, below, refers to any such program or work, and a “work based on the Program” means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification”.) Each licensee is addressed as “you”.

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

2. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a). You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b). You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c). If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

   Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

   In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a). Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, b). Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c). Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

5. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

6. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

7. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

8. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

9. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
10. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

    Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.
11. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

1. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
2. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

**END OF TERMS AND CONDITIONS**

# AG GLOSSARY

**ACL** Access Control List. ACLs can limit network traffic and restrict access to certain users or devices by checking each packet for certain IP or MAC (i.e., Layer 2) information.

**ARP** Address Resolution Protocol converts between IP addresses and MAC (i.e., hardware) addresses. ARP is used to locate the MAC address corresponding to a given IP address. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next.

**BOOTP** Boot Protocol. BOOTP is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

**CoS** Class of Service is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence bit, or DSCP priority bit.

**DHCP** Dynamic Host Control Protocol. Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

**DHCP Option 82** A relay option for sending information about the requesting client (or an intermediate relay agent) in the DHCP request packets forwarded by the switch and in reply packets sent back from the DHCP server. This information can be used by DHCP servers to assign fixed IP addresses, or set other services or policies for clients.

**DHCP Snooping** A technique used to enhance network security by snooping on DHCP server messages to track the physical location of hosts, ensure that hosts only use the IP addresses assigned to them, and ensure that only authorized DHCP servers are accessible.

**DIFFSERV** Differentiated Services provides quality of service on large networks by employing a well-defined set of building blocks from which a variety of aggregate forwarding behaviors may be built. Each packet carries information (DS byte) used by each hop to give it a particular forwarding treatment, or per-hop behavior, at each network node. DiffServ allocates different levels of service to users on the network with mechanisms such as traffic meters, shapers/droppers, packet markers at the boundaries of the network.

**DNS** Domain Name Service. A system used for translating host names for network nodes into IP addresses.

**DSCP** Differentiated Services Code Point Service. DSCP uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.

**EAPOL** Extensible Authentication Protocol over LAN. EAPOL is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A user name and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1X Port Authentication standard.

**EUI** Extended Universal Identifier is an address format used by IPv6 to identify the host portion of the network address. The interface identifier in EUI compatible addresses is based on the link-layer (MAC) address of an interface. Interface identifiers used in global unicast and other IPv6 address types are 64 bits long and may be constructed in the EUI-64 format. The modified EUI-64 format interface ID is derived from a 48-bit link-layer address by inserting the hexadecimal number FFFE between the upper three bytes (OUI field) and the lower 3 bytes (serial number) of the link layer address. To ensure that the chosen address is from a unique Ethernet MAC address, the 7th bit in the high-order byte is set to 1 (equivalent to the IEEE Global/Local bit) to indicate the uniqueness of the 48-bit address.

**GARP** Generic Attribute Registration Protocol. GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.

**GMRP** Generic Multicast Registration Protocol. GMRP allows network devices to register end stations with multicast groups. GMRP requires that any participating network devices or end stations comply with the IEEE 802.1p standard.

**GVRP** GARP VLAN Registration Protocol. Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

**IEEE 802.1D** Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

**IEEE 802.1Q** VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

**IEEE 802.1P** An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

**IEEE 802.1S** An IEEE standard for the Multiple Spanning Tree Protocol (MSTP) which provides independent spanning trees for VLAN groups.

**IEEE 802.1W** An IEEE standard for the Rapid Spanning Tree Protocol (RSTP) which reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard. (Now incorporated in IEEE 802.1D-2004)

**IEEE 802.1X** Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

**IEEE 802.3AC** Defines frame extensions for VLAN tagging.

**IEEE 802.3X** Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links. (Now incorporated in IEEE 802.3-2002)

**ICMP** Internet Control Message Protocol is a network layer protocol that reports errors in processing IP packets. ICMP is also used by routers to feed back information about better routing choices.

**IGMP** Internet Group Management Protocol. A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast switch/router on a given subnetwork, one of the devices is made the “querier” and assumes responsibility for keeping track of group membership.

**IGMP PROXY** Proxies multicast group membership information onto the upstream interface based on IGMP messages monitored on downstream interfaces, and forwards multicast traffic based on that information. There is no need for multicast routing protocols in an simple tree that uses IGMP Proxy.

**IGMP QUERY** On each subnetwork, one IGMP-capable device will act as the querier — that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

**IGMP SNOOPING** Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

**IN-BAND MANAGEMENT** Management of the network from a station attached directly to the network.

**IP MULTICAST FILTERING** A process whereby this switch can pass multicast traffic along to participating hosts.

**IP PRECEDENCE** The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The eight values are mapped one-to-one to the Class of Service categories by default, but may be configured differently to suit the requirements for specific network applications.

**LACP** Link Aggregation Control Protocol. Allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

**LAYER 2** Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

**LAYER 3** Network layer in the ISO 7-Layer Data Communications Protocol. This layer handles the routing functions for data moving from one open system to another.

**LINK AGGREGATION** See Port Trunk.

**LLDP** Link Layer Discovery Protocol is used to discover basic information about neighboring devices in the local broadcast domain by using periodic broadcasts to advertise information such as device identification, capabilities and configuration settings.

**MD5** MD5 Message-Digest is an algorithm that is used to create digital signatures. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

**MIB** Management Information Base. An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

**MRD** Multicast Router Discovery is a A protocol used by IGMP snooping and multicast routing devices to discover which interfaces are attached to multicast routers. This process allows IGMP-enabled devices to determine where to send multicast source and group membership messages.

**MSTP** Multiple Spanning Tree Protocol can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group.

**MULTICAST SWITCHING** A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

**MVR** Multicast VLAN Registration is a method of using a single network-wide multicast VLAN to transmit common services, such as such as television channels or video-on-demand, across a service-provider's network. MVR simplifies the configuration of multicast services by using a common VLAN for distribution, while still preserving security and data isolation for subscribers residing in both the MVR VLAN and other standard or

private VLAN groups.

**NTP** Network Time Protocol provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

**OSPF** Open Shortest Path First is a link-state routing protocol that functions better over a larger network such as the Internet, as opposed to distance-vector routing protocols such as RIP. It includes features such as unlimited hop count, authentication of routing updates, and Variable Length Subnet Masks (VLSM).

**OUT-OF-BAND MANAGEMENT** Management of the network from a station not attached to the network.

**PORT AUTHENTICATION** *See IEEE 802.1X.*

**PORT MIRRORING** A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

**PORT TRUNK** Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

**PRIVATE VLANS** Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports.

**QINQ** QinQ tunneling is designed for service providers carrying traffic for multiple customers across their networks. It is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs.

**QOS** Quality of Service. QoS refers to the capability of a network to provide better service to selected traffic flows using features such as data prioritization, queuing, congestion avoidance and traffic shaping. These features effectively provide preferential treatment to specific flows either by raising the priority of one flow or limiting the priority of another flow.

**RADIUS** Remote Authentication Dial-in User Service. RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

**RIP** Routing Information Protocol seeks to find the shortest route to another device by minimizing the distance-vector, or hop count, which serves as a rough estimate of transmission cost. RIP-2 is a compatible upgrade to RIP. It adds useful capabilities for subnet routing, authentication, and multicast transmissions.

**RMON** Remote Monitoring. RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

**RSTP** Rapid Spanning Tree Protocol. RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.

**SMTP** Simple Mail Transfer Protocol is a standard host-to-host mail transport protocol that operates over TCP, port 25.

**SNMP** Simple Network Management Protocol. The application protocol in the Internet suite of protocols which offers network management services.

**SNTP** Simple Network Time Protocol allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

**SSH** Secure Shell is a secure replacement for remote access functions, including Telnet. SSH can authenticate users with a cryptographic key, and encrypt data connections between management clients and the switch.

**STA** Spanning Tree Algorithm is a technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

**TACACS+** Terminal Access Controller Access Control System Plus. TACACS+ is a logon authentication protocol that uses software running on a central server to control access to TACACS-compliant devices on the network.

**TCP/IP** Transmission Control Protocol/Internet Protocol. Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

**TELNET** Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

**TFTP** Trivial File Transfer Protocol. A TCP/IP protocol commonly used for software downloads.

**UDP** User Datagram Protocol. UDP provides a datagram mode for packet-switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

**UTC** Universal Time Coordinate. UTC is a time scale that couples Greenwich Mean Time (based solely on the Earth's rotation rate) with highly accurate atomic time. The UTC does not have daylight saving time.

**VLAN** Virtual LAN. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

**VRRP** Virtual Router Redundancy Protocol uses a virtual IP address to support a primary router and multiple backup routers. The backups can be configured to take over the workload if the master fails or to load share the traffic. The primary goal of VRRP is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

**XMODEM** A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

# INDEX

## NUMERICS



## A



## B



## C

# D



# E

## M



## N



## O

## P

## Q



## R